Graduate Texts in Mathematics

John D. Dixon
Brian Mortimer

Permutation Groups

Springer

Graduate Texts in Mathematics 163

Editorial Board
S. Axler F.W. Gehring P.R. Halmos

Springer-Science+Business Media, LLC

Graduate Texts in Mathematics

1 Takeuti/Zaring. Introduction to Axiomatic Set Theory. 2nd ed.
2 Oxtoby. Measure and Category. 2nd ed.
3 Schaefer. Topological Vector Spaces.
4 Hilton/Stammbach. A Course in Homological Algebra.
5 Mac Lane. Categories for the Working Mathematician.
6 Hughes/Piper. Projective Planes.
7 Serre. A Course in Arithmetic.
8 Takeuti/Zaring. Axiomatic Set Theory.
9 Humphreys. Introduction to Lie Algebras and Representation Theory.
10 Cohen. A Course in Simple Homotopy Theory.
11 Conway. Functions of One Complex Variable I. 2nd ed.
12 Beals. Advanced Mathematical Analysis.
13 Anderson/Fuller. Rings and Categories of Modules. 2nd ed.
14 Golubitsky/Guillemin. Stable Mappings and Their Singularities.
15 Berberian. Lectures in Functional Analysis and Operator Theory.
16 Winter. The Structure of Fields.
17 Rosenblatt. Random Processes. 2nd ed.
18 Halmos. Measure Theory.
19 Halmos. A Hilbert Space Problem Book. 2nd ed.
20 Husemoller. Fibre Bundles. 3rd ed.
21 Humphreys. Linear Algebraic Groups.
22 Barnes/Mack. An Algebraic Introduction to Mathematical Logic.
23 Greub. Linear Algebra. 4th ed.
24 Holmes. Geometric Functional Analysis and Its Applications.
25 Hewitt/Stromberg. Real and Abstract Analysis.
26 Manes. Algebraic Theories.
27 Kelley. General Topology.
28 Zariski/Samuel. Commutative Algebra. Vol.I.
29 Zariski/Samuel. Commutative Algebra. Vol.II.
30 Jacobson. Lectures in Abstract Algebra I. Basic Concepts.
31 Jacobson. Lectures in Abstract Algebra II. Linear Algebra.
32 Jacobson. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 Hirsch. Differential Topology.
34 Spitzer. Principles of Random Walk. 2nd ed.
35 Wermer. Banach Algebras and Several Complex Variables. 2nd ed.
36 Kelley/Namioka et al. Linear Topological Spaces.
37 Monk. Mathematical Logic.
38 Grauert/Fritzsche. Several Complex Variables.
39 Arveson. An Invitation to C^*-Algebras.
40 Kemeny/Snell/Knapp. Denumerable Markov Chains. 2nd ed.
41 Apostol. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 Serre. Linear Representations of Finite Groups.
43 Gillman/Jerison. Rings of Continuous Functions.
44 Kendig. Elementary Algebraic Geometry.
45 Loève. Probability Theory I. 4th ed.
46 Loève. Probability Theory II. 4th ed.
47 Moise. Geometric Topology in Dimensions 2 and 3.
48 Sachs/Wu. General Relativity for Mathematicians.
49 Gruenberg/Weir. Linear Geometry. 2nd ed.
50 Edwards. Fermat's Last Theorem.
51 Klingenberg. A Course in Differential Geometry.
52 Hartshorne. Algebraic Geometry.
53 Manin. A Course in Mathematical Logic.
54 Graver/Watkins. Combinatorics with Emphasis on the Theory of Graphs.
55 Brown/Pearcy. Introduction to Operator Theory I: Elements of Functional Analysis.
56 Massey. Algebraic Topology: An Introduction.
57 Crowell/Fox. Introduction to Knot Theory.
58 Koblitz. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 Lang. Cyclotomic Fields.
60 Arnold. Mathematical Methods in Classical Mechanics. 2nd ed.

continued after index

John D. Dixon
Brian Mortimer

Permutation Groups

Springer

John D. Dixon
Brian Mortimer
Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6

Editorial Board

S. Axler
Department of Mathematics
Michigan State University
East Lansing, MI 48824
USA

F.W. Gehring
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

P.R. Halmos
Department of Mathematics
Santa Clara University
Santa Clara, CA 95053
USA

With 10 Figures

Mathematics Subject Classification (1991): 20-01, 20Bxx

Library of Congress Cataloging-in-Publication Data
Dixon, John D.
Permutation groups / John D. Dixon, Brian Mortimer.
p. cm. — (Graduate texts in mathematics ; 163)
Includes bibliographical references and index.
ISBN 978-1-4612-6885-7 ISBN 978-1-4612-0731-3 (eBook)
DOI 10.1007/978-1-4612-0731-3
1. Permutation groups. I. Mortimer, Brian. II. Title.
III. Series.
QA175.D59 1996
512′.2—dc20 95-44880

Printed on acid-free paper.

© 1996 Springer Science+Business Media New York
Originally published by Springer-Verlag New York, Inc in 1996
Softcover reprint of the hardcover 1st edition 1996

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Science+Business Media, LLC), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production managed by Bill Imbornoni; manufacturing supervised by Joe Quatela.
Photocomposed pages prepared from the authors' TeX files.

9 8 7 6 5 4 3 2

ISBN 978-1-4612-6885-7 SPIN 10567787

Preface

Permutation groups arguably form the oldest part of group theory. Their study dates back to the early years of the nineteenth century and, indeed, for a long time groups were always understood to be permutation groups. Although, of course, this is no longer true, permutation groups continue to play an important role in modern group theory through the ubiquity of group actions and the concrete representations which permutation groups provide for abstract groups. Today, both finite and infinite permutation groups are lively topics of research.

In this book we have tried to present something of the sweep of the development of permutation groups, explaining where the problems have come from as well as how they have been solved. Where appropriate we deal with finite and infinite groups together. Some of the theorems we consider arose in the last century or the earlier parts of this century, but most of the book deals with work done over the last few decades. In particular, the kinds of problem in finite permutation groups which can be usefully tackled has completely changed since the classification of finite simple groups was announced in 1979 (see Appendix A). One chapter of this book is devoted to the proof of the pivotal O'Nan–Scott Theorem which links the classification of finite simple groups directly to problems in finite permutation groups. We have described some of the applications of the O'Nan–Scott Theorem, even though in many cases the proofs are too technical for consideration here.

This book is intended as an introduction to permutation groups. It can be used as a text for a graduate or advanced undergraduate level course, or for independent study. The reader should have had a general introduction to group theory, and know about such things as the Sylow theorems, composition series and automorphism groups, but we have kept the prerequisites modest and recall specific facts as needed. Material in the first three chapters of the book is basic, but later chapters can be read largely independently of one another, so the text can be adapted for a variety of courses. An instructor should first cover Chapters 1 to 3 and then select

material from further chapters depending on the interests of the class and the time available.

Our own experiences in learning have led us to take considerable trouble to include a large number of examples and exercises; there are over 600 of the latter. Exercises range from simple to moderately difficult, and include results (often with hints) which are referred to later. As the subject develops, we encourage the reader to accept the invitation of becoming involved in the process of discovery by working through these exercises. Keep in mind Shakespeare's advice: "Things done without example, in their issue are to be fear'd" (*King Henry the Eighth, I.ii.90*).

Although it has been a very active field during the past 20 to 30 years, no general introduction to permutation groups has appeared since H. Wielandt's influential book *Finite Permutation Groups* was published in 1964. This is a pity since the area is both interesting and accessible. Our book makes no attempt to be encyclopedic and some choices have been a little arbitrary, but we have tried to include topics indicative of the current development of the subject. Each chapter ends with a short section of notes and a selection of references to the extensive literature; again there has been no attempt to be exhaustive and many important papers have had to be omitted.

We have personally known a great deal of pleasure as our understanding of this subject has grown. We hope that some of this pleasure is reflected in the book, and will be evident to the reader. A book like this owes a clear debt to the many mathematicians who have contributed to the subject; especially Camille Jordan (whose *Traité de substitutions et des équations algébriques* was the first text book on the subject) and Helmut Wielandt, but also, more personally, to Peter Neumann and Peter Cameron. We thank Bill Kantor, Joachim Neubüser and Laci Pyber who each read parts of an early version of the manuscript and gave useful advice. Although we have taken considerable care over the manuscript, we expect that inevitably some errors will remain; if you find any, we should be grateful to hear from you.

Finally, we thank our families who have continued to support and encourage us in this project over a period of more than a decade.

Acknowledgement. The tables in Appendix B were originally published as Tables 2, 3 and 4 of: John D. Dixon and Brian Mortimer, Primitive permutation groups of degree less than 1000, *Math. Proc. Cambridge Phil. Soc.* 103 (1988) 213–238. They are reprinted with permission of Cambridge University Press.

Contents

Notation

$\mathbb{N}, \mathbb{Z}$	natural numbers and integers
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$	rational, real and complex numbers
$\mathbb{F}_q$	field with q elements
K^d	vector space of dimension d over K
$AG_d(K), AG_d(q)$	affine geometry over K and over $\mathbb{F}_q$
$PG_d(K), PG_d(q)$	projective geometry over K and over $\mathbb{F}_q$
$S(t, k, v)$	Steiner system
$Sym(\Omega), Alt(\Omega)$	symmetric and alternating groups on Ω
S_n, A_n	symmetric and alternating groups of degree n
$FSym(\Omega)$	finitary symmetric group
C_n	cyclic group of order n
$GL_d(K), SL_d(K), \Gamma L_d(K)$	linear groups over K
$AGL_d(K), ASL_d(K), A\Gamma L_d(K)$	affine groups over K
$PGL_d(K), PSL_d(K), P\Gamma L_d(K)$	projective groups over K
$Sp_{2m}(K), Sp_{2m}(2)$	symplectic groups over K
$PGU_3(q), PSU_3(q), P\Gamma U_d(q)$	unitary groups over K
$Sz(2^s)$ and $R(3^s)$	Suzuki and Ree groups
$M_{10}, \ldots, M_{24}$	Mathieu groups
$W_{10}, \ldots, W_{24}$	Witt geometries
$\mathrm{fix}(x), \mathrm{supp}(x)$	set of fixed points and support of x
$\Omega^{\{k\}}, \Omega^{(k)}$	sets of k-subsets and k-tuples from Ω
$\mathrm{Orb}(K, \Delta)$	set of orbits of K on Δ
$\mathrm{Graph}(\Delta)$	orbital graph
$\mathrm{GCD}(m, n)$	greatest common divisor of m and n
$\lfloor x \rfloor$	largest integer $\leq x$
$\|S\|$	cardinality of set S
$\Omega \setminus \Delta$	elements of Ω not in Δ
$\Gamma \ominus \Delta$	symmetric difference of Γ and Δ
$\mathrm{Fun}(\Gamma, \Delta)$	set of functions from Γ to Δ
$\mathrm{Im}(\Phi), \ker(\Phi)$	image and kernel of Φ

$\mathrm{Aut}(X)$	automorphism group of X
$\mathrm{Inn}(G)$	inner automorphism group of G
$\mathrm{Out}(G)$	outer automorphism group of G
$\mathrm{soc}(G)$	socle of G
$N_G(H)$	normalizer of H in G
$C_G(H)$	centralizer of H in G
$H \leq G, N \lhd G$	subgroup, normal subgroup
$G \times H, G^m$	direct product, direct power
$G \rtimes H$	semidirect product
$G\ wr_\Gamma\ H$	wreath product
$G.H, G.n$	an extension of G by H, by C_n
$G : H$	a split extension of G by H

1

The Basic Ideas

1.1 Symmetry

A cube is highly symmetric: there are many ways to rotate or reflect it so that it moves onto itself. A cube with labeled vertices is shown in Fig. 1.1. For example, we can rotate it by 90° about an axis through the centres of opposite faces, or reflect it in the plane through a pair of opposite edges. Each of these "symmetries" of the cube permutes the eight vertices in a particular way, and knowing what happens to the vertices is enough to tell us what the whole motion is. The symmetries of the cube thus correspond to a subgroup of permutations of the set of vertices, and this group, an algebraic object, records information about the geometric symmetries.

Turn now to an algebraic example. The polynomial $X^5 - X + 1$ is a real polynomial with five distinct complex roots: one real and four nonreal. As is well-known, nonreal roots of a real polynomial appear in pairs of complex conjugates, so the action of complex conjugation leaves the real root fixed and permutes the nonreal roots in pairs. More generally, any automorphism of the field of complex numbers induces a permutation on the set of roots, and the set of all such permutations forms a group which is called the *Galois group* of the polynomial. Calculating Galois groups can be quite difficult, but in the case of $X^5 - X + 1$ it can be shown to be the full symmetric group of all 120 permutations on the roots. On the other

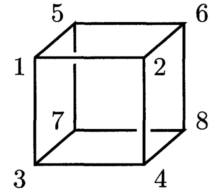


FIGURE 1.1. A labeled cube.

hand, the polynomial $X^5 - 2$ has a group of order 20 as its Galois group. The algebraic symmetries of the polynomial described by the Galois group are not at all obvious.

The development of the theory of permutations and permutation groups over the last two centuries was originally motivated by use of permutation groups as a tool for exploring geometrical, algebraic and combinatorial symmetries. Naturally, the study of permutation groups gave rise to problems of intrinsic interest beyond this initial focus on concrete symmetries, and historically this led to the concept of an abstract group at the end of the nineteenth century.

1.2 Symmetric Groups

Let Ω be an arbitrary nonempty set; we shall often refer to its elements as *points.* A bijection (a one-to-one, onto mapping) of Ω onto itself is called a *permutation* of Ω. The set of all permutations of Ω forms a group, under composition of mappings, called the *symmetric group* on Ω. We shall denote this group by $Sym(\Omega)$ (other common notations are S_Ω and S^Ω), and write S_n to denote the special group $Sym(\Omega)$ when n is a positive integer and $\Omega = \{1, 2, \ldots, n\}$. A *permutation group* is just a subgroup of a symmetric group. If Ω and Ω' are two nonempty sets of the same cardinality (that is, there is a bijection $\alpha \mapsto \alpha'$ from Ω onto Ω') then the group $Sym(\Omega)$ is isomorphic to the group $Sym(\Omega')$ via the mapping $x \mapsto x'$ defined by:

$$x' \text{ takes } \alpha' \text{ to } \beta' \text{ when } x \text{ takes } \alpha \text{ to } \beta.$$

In particular, $Sym(\Omega) \cong S_n$ whenever $|\Omega| = n$.

Exercises

1.2.1 Show in detail that the mapping described above does give an isomorphism from $Sym(\Omega)$ onto $Sym(\Omega')$.

1.2.2 Prove that if Ω is finite and $|\Omega| = n$, then $|Sym(\Omega)| = n!$.

1.2.3 (For those who know something about infinite cardinalities.) Show that if Ω is infinite, then $|Sym(\Omega)| = 2^{|\Omega|}$. In particular, $Sym(\mathbb{N})$ has uncountably many elements when $\mathbb{N}$ is the set of natural numbers.

There are two common ways in which permutations are written (at least for the finite case). First of all, the mapping $x : \Omega \to \Omega$ may be written out explicitly in the form

$$x = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix}$$

where the top row is some enumeration of the points of Ω and β_i is the image of α_i under x for each i. The other notation is to write x as a

product of disjoint cycles. A permutation $c \in Sym(\Omega)$ is called an *r-cycle* ($r = 1, 2, \ldots$) if for r distinct points $\gamma_1, \gamma_2, \ldots, \gamma_r$ of Ω, c maps γ_i onto $\gamma_{i+1} (i = 1, \ldots, r-1)$, maps γ_r onto γ_1, and leaves all other points fixed; and c is called an *infinite cycle* if for some doubly infinite sequence $\gamma_i (i \in \mathbb{Z})$, c maps γ_i onto γ_{i+1} for each i and leaves all other points fixed. The second common way to specify a permutation is to write x as a product of disjoint cycles, where by *disjoint* we mean that no two cycles move a common point (this product is only a formal product in the case that Ω is infinite). It is a general result (see Exercise 1.2.5 below) that every permutation can be written in essentially one way in this form.

EXAMPLE 1.2.1. Let Ω be the finite field of 7 elements consisting of $\{0, 1, \ldots, 6\}$ with addition and multiplication taken modulo 7. Then the mapping $\alpha \mapsto 4\alpha + 1$ defines a permutation of Ω. This permutation can be written

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 0 & 4 \end{pmatrix}$$

or as a product of disjoint cycles

$$(015)(2)(364) = (2)(015)(643) = \ldots = (015)(364)$$

EXAMPLE 1.2.2. Let $\Omega = \mathbb{Q}$ (the rational numbers). Then the mapping $\alpha \mapsto 2\alpha$ is a permutation of Ω. This permutation fixes the point 0, and the remaining points lie in infinite cycles of the form

$$(\ldots, \alpha 2^{-2}, \alpha 2^{-1}, \alpha, \alpha 2^1, \alpha 2^2, \ldots).$$

Our convention is to consider permutations as functions acting on the right. This means that a product xy of permutations should be read as: first apply x and then y (some authors follow the opposite convention). For example, $(142)(356)(4123) = (1)(2)(3564)$.

Exercises

1.2.4 Show that an r-cycle $(\alpha_1 \ldots \alpha_r)$ is equal to an s-cycle $(\beta_1 \ldots \beta_s)$ on the same set Ω if and only if $r = s$ and for some h we have $\alpha_{i+h} = \beta_i$ for each i where the indices are taken modulo r. Show that two infinite cycles $(\ldots \alpha_{-1}\alpha_0\alpha_1 \ldots)$ and $(\ldots \beta_{-1}\beta_0\beta_1 \ldots)$ on the same set are equal if and only if for some h, $\alpha_{i+h} = \beta_i$ for all i.

1.2.5 Prove that each permutation $x \in Sym(\Omega)$ can be written as a product of disjoint cycles. Show that this product is unique up to the order in which the cycles appear in the product and the inclusion or exclusion of 1-cycles (corresponding to the points left fixed by x). [*Hint:* Two symbols, say α and β, will lie in the same cycle for x if and only if some power of x maps α onto β. This latter condition defines an equivalence relation on Ω and hence a partition of Ω into

disjoint subsets. Note that when Ω is infinite, x may have infinite cycles and may also have infinitely many cycles. In the latter case the product as disjoint cycles has to be interpreted suitably.]

1.2.6 Suppose that x and y are permutations in $Sym(\Omega)$, and that $y = c_1c_2\ldots$ as a product of disjoint cycles. Show that $x^{-1}yx = c_1'c_2'\ldots$ where each cycle c_i of y is replaced by a cycle c_i' of the same length, and each point in c_i is replaced in c_i' by its image under x. In particular, if α_i' is the image of α_i under x then we have

$$x^{-1}(\alpha_1,\ldots,\alpha_k)x = (\alpha_1',\ldots,\alpha_k').$$

1.2.7 Show that two permutations $x, y \in Sym(\Omega)$ are conjugate in $Sym(\Omega)$ if and only if they have the same number of cycles of each type (including 1-cycles). Give an example of two infinite cycles in $Sym(\mathbb{N})$ which are not conjugate.

1.2.8 If the permutation x is a product of k disjoint cycles of finite lengths $m_1,\ldots,m_k$, show that the order of x as a group element is the least common multiple of these lengths. What is the largest order of an element in S_{20}?

1.2.9 Find the cycle decomposition of the permutation induced by the action of complex conjugation on the set of roots of $X^5 - X + 1$.

1.2.10 Which permutations of the set $\Omega := \{X_1, X_2, X_3, X_4\}$ leave the polynomial $X_1 + X_2 - X_3 - X_4$ invariant? Find a polynomial in these variables which is left invariant under all permutations in the group $\langle (X_1X_2X_3X_4), (X_2X_4)\rangle$ but not by all of $Sym(\Omega)$.

1.2.11 For each i, $2 \le i \le n$, let $L_i = \{(1,i),(2,i),\ldots,(i-1,i), I\}$ where I is the identity element of S_n. Show that each $x \in S_n$ can be written uniquely as a product $x = x_2x_3\ldots x_n$ with $x_i \in L_i$. (This is the basis for a technique to generate random elements of S_n with uniform distribution.)

1.2.12 Let $s(n,k)$ denote the number of permutations in S_n which have exactly k cycles (including 1-cycles). Show that

$$\sum_{k=1}^{n} s(n,k)X^k = X(X+1)\ldots(X+n-1).$$

(The $s(n,k)$ are known as "Stirling numbers of the first kind".)

1.2.13 Let $a(n,m)$ denote the number of permutations $x \in S_n$ such that $x^m = 1$ (with $a(0,m) = 1$). Show that

$$\sum_{n=0}^{\infty} \frac{a(n,m)}{n!}X^n = \exp\left\{\sum_{d|m} \frac{X^d}{d}\right\}.$$

1.2.14 Find necessary and sufficient conditions on the pair i, j in order that $\langle (12\ldots n), (ij)\rangle = S_n$.

1.2.15 Show that for all i, $1 < i \le n$, $\langle (23\ldots n), (1i)\rangle = S_n$.

1.2.16 Let $n \geq 2$, and let T be the set of all permutations in S_n of the form

$$t_k := \prod_{1 \leq i \leq k/2} (i \;\; k{-}i) \quad \text{for } k = 3, 4, \ldots, n+1.$$

(i) Show that T generates S_n and that each $x \in S_n$ can be written as a product of $2n - 3$ or fewer elements from T.

(ii) (Unsolved problem) Find the least integer f_n such that every $x \in S_n$ can be written as a product of at most f_n elements from T.

1.3 Group Actions

The examples described in Sect. 1.1 show how permutation groups are induced by the action of groups of geometrical symmetries and field automorphisms on specified sets. This idea of a group acting on a set can be formalized as follows.

Let G be a group and Ω be a nonempty set, and suppose that for each $\alpha \in \Omega$ and each $x \in G$ we have defined an element of Ω denoted by α^x (in other words, $(\alpha, x) \mapsto \alpha^x$ is a function of $\Omega \times G$ into Ω). Then we say that this defines an *action* of G on Ω (or G *acts* on Ω) if we have:

(i) $\alpha^1 = \alpha$ for all $\alpha \in \Omega$ (where 1 denotes the identity element of G); and
(ii) $(\alpha^x)^y = \alpha^{xy}$ for all $\alpha \in \Omega$ and all $x, y \in G$.

Whenever we speak about a group acting on a set we shall implicitly assume that the set is nonempty.

EXAMPLE 1.3.1. The group of symmetries of the cube acts on a variety of sets including: the set of eight vertices, the set of six faces, the set of twelve edges, and the set of four principal diagonals. In each case properties (i) and (ii) are readily verified.

EXAMPLE 1.3.2. Every subgroup G of $Sym(\Omega)$ acts naturally on Ω where α^x is simply the image of α under the permutation x. Except when explicitly stated otherwise, we shall assume that this is the action we are dealing with whenever we have a group of permutations.

If a group G acts on a (nonempty) set Ω, then to each element $x \in G$ we can associate a mapping $\overline{x}$ of Ω into itself, namely, $\alpha \mapsto \alpha^x$. The mapping $\overline{x}$ is a bijection since it has $\overline{x^{-1}}$ as its inverse (using properties (i) and (ii)); hence we have a mapping $\rho : G \to Sym(\Omega)$ given by $\rho(x) := \overline{x}$. Moreover, using (i) and (ii) again, we see that ρ is a group homomorphism since for all $\alpha \in \Omega$ and all $x, y \in G$, the image of α under $\overline{xy}$ is the same as its image under the product $\overline{x}\ \overline{y}$. In general, any homomorphism of G

into $Sym(\Omega)$ is called a *(permutation) representation* of G on Ω. Hence, we see that each action of G on Ω gives rise to a representation of G on Ω. Conversely, representations correspond to actions (see Exercise 1.3.1), so we may think of group actions and permutation representations as different ways of describing the same situation.

The following concepts related to a group action will be referred to repeatedly. The *degree* of an action (or a representation) is the size of Ω. The *kernel* of the action is the kernel ($\ker \rho$) of the representation ρ; and an action (or representation) is *faithful* when $\ker \rho = 1$. The "first homomorphism theorem" shows that, when the action is faithful, the image $\operatorname{Im} \rho$ is isomorphic to G.

In some applications the relevant action is of the group acting on a set directly related to the group itself, as the following examples illustrate.

EXAMPLE 1.3.3. (Cayley representation) For any group G we can take $\Omega := G$ and define an action by *right multiplication*: $a^x := ax$ with $a, ax \in \Omega$ and $x \in G$. (Check that this is an action!). The corresponding representation of G into $Sym(G)$ is called the *(right) regular representation*. It is faithful since the kernel

$$\{x \in G \mid a^x = a \text{ for all } a \in \Omega\}$$

equals 1. This shows that every group is isomorphic to a permutation group.

EXAMPLE 1.3.4. (Action on right cosets) For any group G and any subgroup H of G we can take $\Gamma_H := \{Ha \mid a \in G\}$ as the set of right cosets of H in G, and define an action of G on Γ_H by right multiplication: $(Ha)^x := Hax$ with $Ha, Hax \in \Gamma_H$ and $x \in G$. We denote the corresponding representation of G on Γ_H by ρ_H. Since $Hax = Ha \iff x \in a^{-1}Ha$, we have

$$\ker \rho_H = \bigcap_{a \in G} a^{-1}Ha.$$

In general, ρ_H is not faithful (see Exercise 1.3.3).

EXAMPLE 1.3.5. Suppose that G and H are both subgroups of a group K and that G normalizes H. Then we can define an action of G on H by *conjugation*: $a^x := x^{-1}ax$ with $a, x^{-1}ax \in H$ and $x \in G$. In this case the kernel of the corresponding representation is the *centralizer* of H in G:

$$C_G(H) := \{x \in G \mid ax = xa \text{ for all } a \in H\}.$$

The most common situation where this action occurs is when $H = G$ or $H \lhd G$ (that is, H is a normal subgroup of G).

Exercises

1.3.1 Let $\rho : G \to Sym(\Omega)$ be a representation of the group G on the set Ω. Show that this defines an action of G on Ω by setting $\alpha^x := \alpha^{\rho(x)}$ for all $\alpha \in \Omega$ and $x \in G$, and that ρ is the representation which corresponds to this action.

1.3.2 Explain why we do not usually get an action of a group G on itself by defining $a^x := xa$. Show, however, that $a^x := x^{-1}a$ does give an action of G on itself (called the *left regular representation* of G. Similarly, show how to define an action of a group on the set of left cosets aH $(a \in G)$ of a subgroup H.

1.3.3 Show that the kernel of ρ_H in Example 1.3.4 is equal to the largest normal subgroup of G contained in the subgroup H.

1.3.4 Use the previous exercise to prove that if G is a group with a subgroup H of finite index n, then G has a normal subgroup K contained in H whose index in G is finite and divides $n!$. In particular, if H has index 2 then H is normal in G.

1.3.5 Let G be a finite group, and let p be the smallest prime which divides the order of G. If G has a subgroup H of index p, show that H must be normal in G. In particular, in a finite p-group (that is, a group of order p^k for some prime p) any subgroup of index p is normal. [*Hint:* Use the previous exercise.]

1.3.6 (Number theory application) Let p be a prime congruent to $1 \pmod 4$, and consider the set

$$\Omega := \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}.$$

Show that the mapping

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

is a permutation of order 2 on Ω with exactly one fixed point. Conclude that the permutation $(x, y, z) \mapsto (x, z, y)$ must also have at least one fixed point, and so $x^2 + 4y^2 = p$ for some $x, y \in \mathbb{N}$.

1.4 Orbits and Stabilizers

When a group G acts on a set Ω, a typical point α is moved by elements of G to various other points. The set of these images is called the *orbit* of α under G, and we denote it by

$$\alpha^G := \{\alpha^x \mid x \in G\}.$$

A kind of dual role is played by the set of elements in G which fix a specified point α. This is called the *stabilizer* of α in G and is denoted

$$G_\alpha := \{x \in G \mid \alpha^x = \alpha\}.$$

The important properties of these objects are summarized in the following theorem.

Theorem 1.4A. *Suppose that G is a group acting on a set Ω and that $x, y \in G$ and $\alpha, \beta \in \Omega$. Then:*

(i) *Two orbits α^G and β^G are either equal (as sets) or disjoint, so the set of all orbits is a partition of Ω into mutually disjoint subsets.*

(ii) *The stabilizer G_α is a subgroup of G and $G_\beta = x^{-1}G_\alpha x$ whenever $\beta = \alpha^x$. Moreover, $\alpha^x = \alpha^y \iff G_\alpha x = G_\alpha y$.*

(iii) *(The orbit-stabilizer property) $|\alpha^G| = |G : G_\alpha|$ for all $\alpha \in \Omega$. In particular, if G is finite then $|\alpha^G|\ |G_\alpha| = |G|$.*

PROOF. If $\delta \in \alpha^G$ then $\delta = \alpha^u$ for some $u \in$ G. Since ux runs over the elements of G as x runs over G, $\delta^G = \{\delta^x \mid x \in G\} = \{\alpha^{ux} \mid x \in G\} = \alpha^G$. Hence, if α^G and β^G have any element δ in common, then $\alpha^G = \delta^G = \beta^G$. Since every element $\alpha \in \Omega$ lies in at least one orbit (namely, α^G), this proves (i).

Clearly $1 \in G_\alpha$, and whenever $x, y \in G_\alpha$ then $xy^{-1} \in G_\alpha$. Thus G_α is a subgroup. If $\beta = \alpha^x$ then we also have:

$$y \in G_\beta \iff \alpha^{xy} = \alpha^x \iff xyx^{-1} \in G_\alpha$$

and so $x^{-1}G_\alpha x = G_\beta$. Finally,

$$\alpha^x = \alpha^y \iff \alpha^{xy^{-1}} = \alpha \iff xy^{-1} \in G_\alpha \iff G_\alpha x = G_\alpha y$$

and so (ii) is proved. Now (iii) follows immediately since (ii) shows that the distinct points in α^G are in bijective correspondence with the right cosets of G_α in G, and for finite groups $|G : G_\alpha| = |G| \,/\, |G_\alpha|$. □

A group G acting on a set Ω is said to be *transitive* on Ω if it has only one orbit, and so $\alpha^G = \Omega$ for all $\alpha \in \Omega$. Equivalently, G is transitive if for every pair of points $\alpha, \beta \in \Omega$ there exists $x \in G$ such that $\alpha^x = \beta$. A group which is not transitive is called *intransitive.* A group G acting transitively on a set Ω is said to act *regularly* if $G_\alpha = 1$ for each $\alpha \in \Omega$ (equivalently, only the identity fixes any point). The previous theorem then has the following immediate corollary.

Corollary 1.4A. *Suppose that G is transitive in its action on the set Ω. Then:*

(i) *The stabilizers G_α $(\alpha \in \Omega)$ form a single conjugacy class of subgroups of G.*

(ii) *The index* $|G : G_\alpha| = |\Omega|$ *for each* α.
(iii) *If* G *is finite then the action of* G *is regular* $\iff |G| = |\Omega|$.

EXAMPLE 1.4.1. We illustrate these concepts by calculating the order of the group G of symmetries of the cube (Sect.1.1). Consider the action of G on the set Ω of vertices labelled as in Fig. 1.1. If x denotes the rotation of the cube through an angle of 90° around an axis through the midpoints of the front and back faces, then the corresponding permutation $\overline{x}$ induced on Ω is $(1342)(5786)$. A similar rotation y through a vertical axis induces the permutation $\overline{y} = (1265)(3487)$. Thus the orbits of the subgroup $\langle x\rangle$ are $1^{\langle x\rangle} = \{1,3,4,2\}$ and $5^{\langle x\rangle} = \{5,7,8,6\}$ and, similarly, $\langle y\rangle$ has orbits $\{1,2,6,5\}$ and $\{3,4,8,7\}$. Since $G \geq \langle x, y\rangle$, the group G itself has a single orbit and so is transitive on Ω. The orbit-stabilizer property now shows that $|G : G_1| = |\Omega| = 8$.

Next consider the action of the subgroup G_1. Any symmetry of the cube which fixes vertex 1 must also fix the opposite vertex 8, and map the vertices 2, 3 and 5 amongst themselves. The rotation z of 120° about the axis through vertices 1 and 8 induces the permutation $\overline{z} = (1)(253)(467)(8) = (253)(467)$ on Ω and lies in G_1, so $\{2,5,3\}$ is an orbit for G_1. Thus the stabilizer G_{12} of 2 in G_1 satisfies $|G_1 : G_{12}| = 3$ by the orbit-stabilizer property.

Finally, consider the stabilizer of two points G_{12}. Each symmetry which fixes vertices 1 and 2 must also fix vertices 7 and 8, and so G_{12} has a single nontrivial element, namely a reflection w in the plane through vertices 1, 2, 7 and 8 which induces the permutation $\overline{w} = (35)(46)$. Thus we conclude that

$$|G| = |G : G_1|\,|G_1 : G_{12}|\,|G_{12}| = 8 \cdot 3 \cdot 2 = 48.$$

EXAMPLE 1.4.2. Let G be a group and consider the conjugation action of G on itself defined in Example 1.3.5. The orbits in this action are the *conjugacy classes* where two elements $a, b \in G$ lie in the same conjugacy class $\iff x^{-1}ax = b$ for some $x \in G$. The stabilizer of an element $a \in G$ is equal to the centralizer $C_G(a) = \{x \in G \mid ax = xa\}$. The orbit-stabilizer property shows that the size of the conjugacy class containing a is equal to $|G : C_G(a)|$. In particular, if G is finite then every conjugacy class has size dividing $|G|$.

Exercises

1.4.1 Let G be a group acting transitively on a set Ω, H be a subgroup of G and G_α be a point stabilizer of G. Show that $G = G_\alpha H \iff G = HG_\alpha \iff H$ is transitive. In particular, the only transitive subgroup of G containing G_α is G itself. (This fact is frequently useful.)

1.4.2 Show that the action of the group of symmetries of the cube on the set of six faces of the cube is transitive, and deduce that the group of symmetries has a subgroup of index 6.

1.4.3 Let $H = G_1$ be the group of symmetries of the cube which fix vertex 1. What are the orbits of H on the set of 12 edges of the cube?

1.4.4 Calculate the order of the symmetry group of the regular dodecahedron.

1.4.5 Let K be a group. Show that we can define an action of the direct product $K \times K$ on the set K by: $a^{(x,y)} := x^{-1}ay$ for all $a \in K$ and $(x, y) \in K \times K$. Show that this action is transitive and find the stabilizer K_1. When is the action faithful?

1.4.6 Suppose that G is a group acting on the set Ω and H is a subgroup of G, and let Δ be an orbit for H. Show that Δ^x is an orbit for $x^{-1}Hx$ for each $x \in G$. If G is transitive on Ω and $H \lhd G$, show that every orbit of H has the form Δ^x for some $x \in G$.

1.4.7 Let G be a group acting on a set Ω and let p be a prime. Suppose that for each $\alpha \in \Omega$ there is a p-element $x \in G$ such that α is the only point fixed by x. If Ω is finite, show that G is transitive on Ω; and if Ω is infinite, show that G has no finite orbit on Ω. Find an example of a group G with an intransitive action on a set Ω such that for each $\alpha \in \Omega$ there is an element $x \in G$ of order 6 which has α as its unique fixed point. [*Hint:* Take $G = S_3 \times S_3$.]

Exercises

The following exercises illustrate how permutation actions can be used to prove some well-known theorems in the theory of abstract groups. Even if you already know the results, you may find the techniques of interest.

1.4.8 If G is a finite p-group and $G \neq 1$, then its centre $Z(G) \neq 1$. [*Hint:* Use Example 1.4.2 and note that the size of each nontrivial conjugacy class is a multiple of p.]

1.4.9 Generalize Exercise 1.4.8 to show that if G is a finite p-group and $1 \neq H \lhd G$, then $H \cap Z(G) \neq 1$.

1.4.10 If G is a finite p-group and H is a proper subgroup, show that the normalizer $N_G(H)$ of H in G properly contains H. In particular, every maximal subgroup of G is normal in G and has index p. [*Hint:* Use Exercise 1.4.8.]

1.4.11 Let p be a prime, and let G be a finite group of order $p^k m$ where $p \nmid m$. Show that G has a subgroup of order p^k (a *Sylow p-subgroup*). [*Hint:* Consider the action by right multiplication of G on the set Ω of all subsets of G of p^k elements. Show that p does not divide $|\ \Omega\ |$, and so some orbit has length > 1 and not divisible by p. If T lies in this orbit, then the stabilizer $G_T < G$ and has order divisible by p^k, so we can apply induction.]

1.4.12 Let G be a finite group with a Sylow p-subgroup P. If Q is any p-subgroup of G, show that for some $x \in G$ we have $Q \leq x^{-1}Px$.

In particular, any two Sylow p-subgroups of G are conjugate in G. [*Hint:* Consider the action of G on the set of right cosets of P in G (Example 1.3.4). Since p does not divide $|G : P|$, Q must have some orbit of length not divisible by p, and so Q has an orbit of length 1. Thus for some $x \in G$, $PxQ = Px$.]

1.4.13 The number of Sylow p-subgroups of a finite group G is congruent to 1 modulo p. [*Hint:* Let Ω be the set of all Sylow p-subgroups, and let P be one of these. Then P acts on Ω by conjugation, and its nontrivial orbits have lengths which are multiples of p because P is a p-group. Show that the only orbit of length 1 is $\{P\}$.]

1.4.14 (The "Frattini argument") Let G be a group with a finite normal subgroup K and let P be a Sylow p-subgroup of K. Show that $KN_G(P) = G$. [*Hint:* G acts by conjugation on the set of Sylow p-subgroups of K, and K is transitive in this action (Why?).]

1.4.15 Let G be a finite group and $K \lhd G$. If there is no proper subgroup H of G such that $G = KH$, then show that K is nilpotent. [*Hint:* Recall that a finite group is nilpotent when it is a direct product of Sylow subgroups. Use the previous exercise.]

1.4.16 Let Ω be the set of all $n \times n$ matrices over a field F and let $G = GL_n(F) \times GL_n(F)$ where $GL_n(F)$ is the group of all $n \times n$ invertible matrices over F.

(i) Show that there is an action of G on Ω defined by $a^{(x,y)} := x^{\mathrm{T}}ay$ $(a, x^{\mathrm{T}}ay \in \Omega$ and $(x,y) \in G)$ where x^{T} denotes the transpose of x.

(ii) Show that G has exactly $n+1$ orbits on Ω and describe these.

(iii) For a suitably chosen point a from each orbit, describe G_a.

[*Hint:* This exercise is related to well known facts in elementary linear algebra.]

1.4.17 If G is a transitive permutation group of degree $p^k m$ (p prime), and P is a Sylow p-subgroup of G, then each orbit of P has length at least p^k.

1.4.18 Let G be a permutation group of degree n, and suppose that each $x \neq 1$ in G has at most k cycles. If $n > k^2$, show that G acts faithfully on each of its orbits, and that these orbits all have prime lengths. Hence show that G is either cyclic of prime order or nonabelian of order pq for distinct primes p and q. [*Hint:* Show that $p^2 > n$ for each prime p dividing $|G|$.]

1.5 Blocks and Primitivity

Consider again the symmetry group G of the cube (Fig. 1.1) acting on the set of eight vertices. Since each symmetry preserves distances, the pairs $\{1,8\}$, $\{2,7\}$, $\{3,6\}$, and $\{4,5\}$ which correspond to the long diagonals must be permuted amongst themselves by the elements of G; in other words, G acts on the set Σ of these four pairs. For example, if x is the rotation

through 90° around the axis through the centres of the faces at the front and the back of the cube, then $\{1,8\}^x = \{3,6\}$, $\{2,7\}^x = \{1,8\}$, $\{3,6\}^x = \{4,5\}$ and $\{4,5\}^x = \{2,7\}$. Since reflection in the centre of the cube leaves each of these pairs fixed, the action of G on Σ is not faithful.

Exercise

1.5.1 Show that the image of the corresponding representation of G is the full symmetric group S_4.

The phenomenon described above for the symmetries of the cube plays an important role in analysis of group actions and permutation groups. We shall formalize this idea below. In what follows we shall extend the action of G on Ω to subsets of Ω by defining $\Gamma^x := \{\gamma^x \mid \gamma \in \Gamma\}$ for each $\Gamma \subseteq \Omega$.

Let G be a group acting transitively on a set Ω. A nonempty subset Δ of Ω is called a *block* for G if for each $x \in G$ either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$.

EXAMPLE 1.5.1. Every group acting transitively on Ω has Ω and the singletons $\{\alpha\}$ ($\alpha \in \Omega$) as blocks; these are called the *trivial* blocks. Any other block is called *nontrivial*. A block which is minimal in the set of all blocks of size > 1 is called a *minimal* block.

EXAMPLE 1.5.2. In the example at the beginning of this section, the group of symmetries of the cube acting on the set of vertices has the blocks $\{1,8\}, \{2,7\}, \{3,6\}$ and $\{4,5\}$ which are clearly minimal blocks. The sets $\{1,4,6,7\}$ and $\{2,3,5,8\}$ are also (non-minimal) blocks. Can you find other nontrivial blocks?

EXAMPLE 1.5.3. If G acts transitively on Ω, and Δ and Γ are blocks for G containing a common point, then $\Delta \cap \Gamma$ is also a block for G. More, generally, any intersection of blocks containing a common point is again a block.

Exercise

1.5.2 Show that the cyclic group $\langle(123456)\rangle$ acting on $\{1,2,3,4,5,6\}$ has exactly five nontrivial blocks.

The importance of blocks arises from the following observation. Suppose that G acts transitively on Ω and that Δ is a block for G. Put $\Sigma := \{\Delta^x \mid x \in G\}$. Then the sets in Σ form a partition of Ω and each element of Σ is a block for G (see Exercise 1.5.3); we call Σ the *system of blocks* containing Δ. Now G acts on Σ in an obvious way, and this new action may give useful information about G provided Δ is not a trivial block.

Let G be a group which acts transitively on a set Ω. We say that the group is *primitive* if G has no nontrivial blocks on Ω; otherwise G is called *imprimitive*. Note that we only use the terms "primitive" and "imprimitive" with reference to a transitive group.

Exercises

1.5.3 Show that the system of blocks Σ defined above forms a partition of Ω and that each of its elements is a block for G. Describe the action of G on Σ in the cases where Δ is a trivial block.

1.5.4 If G is a group acting on a set Ω then a *G-congruence* on Ω is an equivalence relation $\approx$ on Ω with the property that

$$\alpha \approx \beta \iff \alpha^x \approx \beta^x \quad \text{for all } x \in G.$$

Show that if G acts transitively on Ω and $\approx$ is a G-congruence, then the equivalence classes of $\approx$ form a system of blocks for G. Conversely, if Σ is a system of blocks for G, then the elements of Σ are the equivalence classes for a G-congruence on Ω. What are the G-congruences which correspond to the trivial blocks?

1.5.5 (Separation property) Suppose that G is a group acting transitively on a set Ω with at least two points, and that Δ is a nonempty subset of Ω. Show that Δ is *not* a block $\iff$ for each pair of distinct points $\alpha, \beta \in \Omega$ there exists $x \in G$ such that exactly one of α and β lies in Δ^x. In the case that G is finite, show that the condition can be strengthened to: $\alpha \in \Delta^x$ but $\beta \notin \Delta^x$ for some $x \in G$.

To describe the relation between blocks and subgroups we shall require the following notation which extends the notation for a point-stabilizer. Suppose G is a group acting on a set Ω, and $\Delta \subseteq \Omega$. Then the *pointwise stabilizer* of Δ in G is

$$G_{(\Delta)} := \{x \in G \mid \delta^x = \delta \quad \text{for all } \delta \in \Delta\}$$

and the *setwise stabilizer* of Δ in G is

$$G_{\{\Delta\}} := \{x \in G \mid \Delta^x = \Delta\}.$$

It is readily seen that $G_{\{\Delta\}}$ and $G_{(\Delta)}$ are both subgroups of G and that $G_{(\Delta)} \triangleleft G_{\{\Delta\}}$. Note that $G_{\{\alpha\}} = G_{(\alpha)} = G_\alpha$ for each $\alpha \in \Omega$. More generally, for a finite set $\Delta = \{\alpha_1, \dots, \alpha_k\}$ we shall often write $G_{\alpha_1,\dots,\alpha_k}$ in place of $G_{(\Delta)}$. (You should be warned that many authors use different notations for these subgroups.)

Exercises

1.5.6 If G acts transitively on Ω, and Δ is a block for G, show that $G_{\{\Delta\}}$ acts transitively on Δ.

1.5.7 Let $G \le \mathrm{Sym}(\Omega)$ be a transitive group and let Γ and Δ be finite subsets of Ω. Suppose that $G_{(\Gamma)}$ and $G_{(\Delta)}$ act primitively on $\Omega \setminus \Gamma$ and $\Omega \setminus \Delta$, respectively, and $G = \langle G_{(\Gamma)}, G_{(\Delta)} \rangle$. Show that the group G is primitive.

Theorem 1.5A. *Let G be a group which acts transitively on a set Ω, and let $\alpha \in \Omega$. Let $\mathcal{B}$ be the set of all blocks Δ for G with $\alpha \in \Delta$, and let*

$\mathcal{S}$ denote the set of all subgroups H of G with $G_\alpha \leq H$. Then there is a bijection Ψ of $\mathcal{B}$ onto $\mathcal{S}$ given by $\Psi(\Delta) := G_{\{\Delta\}}$ whose inverse mapping Φ is given by $\Phi(H) := \alpha^H$. The mapping Ψ is order-preserving in the sense that if $\Delta, \Gamma \in \mathcal{B}$ then $\Delta \subseteq \Gamma \iff \Psi(\Delta) \leq \Psi(\Gamma)$.

Remark. Briefly: the partially ordered set $(\mathcal{B}, \subseteq)$ is order-isomorphic with the partially ordered set $(\mathcal{S}, \leq)$.

PROOF. We first show that Ψ maps $\mathcal{B}$ into $\mathcal{S}$. Let $\Delta \in \mathcal{B}$. Then $x \in G_\alpha$ implies that $\alpha \in \Delta \cap \Delta^x$, and so $\Delta = \Delta^x$ because Δ is a block. This shows that each $x \in G_\alpha$ lies in $G_{\{\Delta\}}$. Hence $G_{\{\Delta\}} \supseteq G_\alpha$ for all $\Delta \in \mathcal{B}$ and so Ψ maps $\mathcal{B}$ into $\mathcal{S}$.

We next show that Φ maps $\mathcal{S}$ into $\mathcal{B}$. Let H be a subgroup of G with $G_\alpha \leq H$. Put $\Delta := \alpha^H$, and let $x \in G$. Clearly $\Delta^x = \Delta$ if $x \in H$, and we claim that $\Delta^x \cap \Delta = \emptyset$ otherwise. Indeed if $\Delta^x \cap \Delta \neq \emptyset$, then there exist $u, v \in H$ such that $\alpha^{ux} = \alpha^v$. Then $uxv^{-1} \in G_\alpha$, and so $x \in u^{-1}G_\alpha v \subseteq H$. Thus $\Delta^x \cap \Delta = \emptyset$ whenever $x \notin H$, and so Δ is a block which contains α, and therefore lies in $\mathcal{B}$. Thus Φ maps $\mathcal{S}$ into $\mathcal{B}$. Moreover, since Δ is an orbit for $G_{\{\Delta\}}$(see Exercise 1.5.6), the composite mapping of Ψ followed by Φ is the identity on $\mathcal{B}$.

To prove that Φ and Ψ are inverses it remains to show that the composite of Φ followed by Ψ is the identity on $\mathcal{S}$. Let $H \in \mathcal{S}$, and put $\Delta := \Phi(H) = \alpha^H$. The previous paragraph shows that if $x \in G$, then $\Delta^x = \Delta \iff x \in H$. Thus $H = G_{\{\Delta\}}$ as required. This completes the proof that Φ is the inverse of Ψ.

The statement that Ψ is order-preserving now follows at once. Indeed $G_{\{\Delta\}} \leq G_{\{\Gamma\}}$ implies that the orbits of α under these groups (namely, Δ and Γ) satisfy $\Delta \subseteq \Gamma$. Conversely, if $\Delta \subseteq \Gamma$, then $x \in G_{\{\Delta\}}$ implies that $\Gamma^x \cap \Gamma \neq \emptyset$ and hence $x \in G_{\{\Gamma\}}$ because Γ is a block. Thus $\Delta \subseteq \Gamma$ implies that $G_{\{\Delta\}} \leq G_{\{\Gamma\}}$. This shows that Ψ is order-preserving, and the theorem is proved. □

This theorem leads immediately to the following important result.

Corollary 1.5A. *Let G be a group acting transitively on a set Ω with at least two points. Then G is primitive $\iff$ each point stabilizer G_α is a maximal subgroup of G.*

Since the point stabilizers of a transitive group are all conjugate (see Corollary 1.4A), one of the point stabilizers is maximal only when all of the point stabilizers are maximal. In particular, a regular permutation group is primitive if and only if it has prime degree.

Exercises

1.5.8 Find all blocks containing 1 for the group

$$G = \langle (123456), (26)(35) \rangle \leq S_6.$$

Identify the corresponding subgroups of G containing G_1.

1.5.9 If Δ is a block for a group G and $\alpha \in \Delta$, show that Δ is a union of orbits for G_α. (This is often useful in looking for blocks.)

1.5.10 Let Δ be a nontrivial block for a group G acting on Ω. If $G_{\{\Delta\}}$ acts imprimitively on Δ (see Exercise 1.5.6), and has a block Γ, show that Γ is also a block for G. In particular, Δ is a minimal block (see Example 1.5.1) for $G \iff G_{\{\Delta\}}$ is primitive on Δ.

1.5.11 Let $z \in Sym(\mathbb{Z})$ be the translation defined by $i^z := i + 1$ for all $i \in \mathbb{Z}$, the integers. Show that the blocks for $\langle z \rangle$ containing 0 are precisely the sets of the form $k\mathbb{Z}$ where $k \in \mathbb{Z}$. In particular, $\langle z \rangle$ has no minimal blocks.

1.5.12 Suppose that G is a group acting on a set Ω with the property that for any two ordered pairs (α, β) and (γ, δ) with $\alpha \neq \beta$ and $\gamma \neq \delta$ there exists $x \in G$ such that $\alpha^x = \gamma$ and $\beta^x = \delta$ (such a group is called *2-transitive*). Show that G is primitive.

1.5.13 Let F be a field and let $G \leq Sym(F)$ consist of all permutations of the form $\xi \mapsto \alpha\xi + \beta$ with $\alpha, \beta \in F$ and $\alpha \neq 0$. Show that G is 2-transitive on F. (We shall give more examples of 2-transitive groups in the next chapter and look at them in detail in Chap. 7.)

1.5.14 Let $G \leq S_n$. If G has r orbits, show that G can be generated by a set of at most $n - r$ elements. In particular, every permutation group of degree n can be generated by a set of at most $n - 1$ elements. Give examples of permutation groups of degree $2m$ which cannot be generated by fewer than m elements ($m = 1, 2, \ldots$).

EXAMPLE 1.5.4. Let $\mathcal{T}$ be the infinite trivalent tree. By this we mean that $\mathcal{T}$ is a graph with a countably infinite set of vertices, each vertex is joined by an edge to exactly three other vertices, and the graph has no cycles. (If you are unfamiliar with graphs, you might like to look in Chap. 2 for the appropriate definitions.)

If you start at any vertex of $\mathcal{T}$ then the tree grows out along three edges each of which splits into two and so on. A fragment of the tree is displayed in Fig. 1.2. Any two trees constructed in this way will be isomorphic.

Let A denote the set of all permutations of the vertex set Ω of $\mathcal{T}$ which preserve the structure of the tree in the sense that if $x \in Sym(\Omega)$, then $x \in A \iff$ two vertices α, β are joined by an edge in $\mathcal{T}$ if and only if α^x and β^x are joined by an edge; A is called the automorphism group of $\mathcal{T}$. Since the graph looks the same from each vertex, A acts transitively on Ω. This action is not primitive because Ω can be partitioned into two nontrivial blocks Δ and Δ' (see Exercise 1.5.15). However, these are minimal blocks

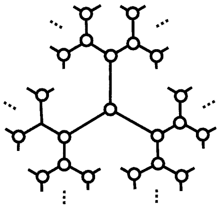


FIGURE 1.2. A fragment of the trivalent tree.

for A, and so $G := A_{\{\Delta\}}$ acts primitively on Δ. (See Exercises 1.5.16 and 1.5.17 for further details.)

Exercises

1.5.15 Define the distance $d(\alpha, \beta)$ between two vertices in the trivalent tree $\mathcal{T}$ to be the number of edges in the shortest path from α to β. Show that:

(i) if $d(\alpha, \beta) = d(\alpha', \beta')$ then there exists $x \in A$ such that $\alpha^x = \alpha'$ and $\beta^x = \beta'$;

(ii) the vertex set Ω can be partitioned into two subsets Δ and Δ' such that the distance between any pair of vertices in the same subset is even;

(iii) the sets Δ and Δ' are blocks for A.

1.5.16 Using the notation of the previous exercise show that Δ and Δ' are the only nontrivial blocks for A, and hence that $G := A_{\{\Delta\}}$ acts primitively on Δ by Exercise 1.5.10. [*Hint:* For any pair of distinct vertices (α, β) there exists $x \in A$ such that $\alpha^x = \alpha$ and $d(\beta, \beta^x) = 2$, thus every nontrivial block contains a pair of points with distance 2.]

1.5.17 With the notation of the previous exercise show that if $\alpha \in \Delta$ then the orbits of G_α on Δ are finite with lengths $1, 6, 24, \ldots$.

1.5.18 Let F be a field, let Ω be the set of all nonzero vectors in the vector space F^3, and let $G = GL_3(F)$ be the group of all invertible 3×3 matrices over F. Consider the action of G on Ω by right (matrix) multiplication: $u^x := ux$ $(u \in \Omega, x \in G)$. Show that:

(i) the action is transitive and faithful;

(ii) the set Δ consisting of those vectors in Ω whose first two entries are 0 is a block; and

(iii) $G_{\{\Delta\}}$ has exactly two orbits on the system of blocks containing Δ.

(This example will be generalized in Sect. 2.8.)

1.5.19 Suppose that the group G acts transitively on Ω and that Γ and Δ are finite subsets of Ω with $|\Gamma| \le |\Delta|$. If $G_{(\Gamma)}$ and $G_{(\Delta)}$ act

transitively on $\Omega \setminus \Gamma$ and $\Omega \setminus \Delta$, respectively, show that $\Gamma^x \subseteq \Delta$ for some $x \in G$. Does the result remain true if Γ and Δ are infinite?

1.5.20 Let G be a solvable transitive subgroup of S_n, and suppose that n can be written as a product of d prime factors. Then G contains a transitive subgroup with at most d generators. [*Hint:* If G is imprimitive, then $G > H > G_\alpha$ for some subgroup H. By induction there exist subgroups L_1, L_2 with d_1 and $d_2 := d - d_1$ generators, respectively, such that $G = HL_1$ and $H = G_\alpha L_2$. Now $\langle L_1, L_2 \rangle$ requires at most d generators.]

1.5.21 Use the preceding exercise to show that every transitive permutation group of prime power degree p^k contains a k-generator transitive p-subgroup.

1.5.22 Let $G \leq Sym(\Omega)$ be a finite primitive group and suppose that G_α has a nontrivial orbit of length d. Show that each subgroup H with $1 < H \leq G_\alpha$ also has a nontrivial orbit of length $\leq d$.

1.6 Permutation Representations and Normal Subgroups

Let G be a group acting on a set Ω. A subset Γ of Ω is *invariant* (or more specifically *G-invariant*) if $\Gamma^x = \Gamma$ for all $x \in G$. Clearly Γ is G-invariant $\Longleftrightarrow$ Γ is a union of orbits of G. In the case that Γ is G-invariant we can consider the restriction of the action of G to Γ and obtain an action of G on Γ. We use the notation $x \mapsto x^\Gamma$ to denote the representation corresponding to this action on Γ (so $x^\Gamma \in Sym(\Gamma)$ is the permutation of Γ associated with the group element x), and write $G^\Gamma := \{x^\Gamma \mid x \in G\}$. The representation $x \mapsto x^\Gamma$ is a homomorphism of G onto G^Γ with kernel $G_{(\Gamma)}$, and so by the "first isomorphism theorem" we have $G/G_{(\Gamma)} \cong G^\Gamma$.

The first theorem of this section describes the relation between the orbits of a group and the orbits of a normal subgroup. To state the result we need one further definition. Two permutation groups, say $G \leq Sym(\Omega)$ and $H \leq Sym(\Omega')$ are called *permutation isomorphic* if there exists a bijection $\lambda : \Omega \to \Omega'$ and a group isomorphism $\psi : G \to H$ such that

$$\lambda(\alpha^x) = \lambda(\alpha)^{\psi(x)} \quad \text{for all } \alpha \in \Omega \text{ and } x \in G.$$

Essentially, this means that the groups are "the same" except for the labelling of the points.

EXAMPLE 1.6.1. Suppose that G is a group acting imprimitively on a set Ω, that H is a normal subgroup of G and that Σ is a system of blocks for G. If $\Delta, \Delta' \in \Sigma$, then $H^\Delta \leq \mathrm{Sym}(\Delta)$ and $H^{\Delta'} \leq Sym(\Delta')$ are permutation isomorphic. Indeed, since Σ is a system of blocks we know that $\Delta' = \Delta^c$ for some $c \in G$, and then we can define a bijection λ of Δ

onto Δ' by $\lambda(\delta) := \delta^c$. Now we claim that we can define an isomorphism $\psi : H^\Delta \to H^{\Delta'}$ by $\psi(x^\Delta) := (c^{-1}xc)^{\Delta'}$. First, ψ is well-defined and injective since for all $x, y \in H$ we have $x^\Delta = y^\Delta \iff xy^{-1} \in H_{(\Delta)} \iff c^{-1}(xy^{-1})c \in H_{(\Delta')} \iff (c^{-1}xc)^{\Delta'} = (c^{-1}yc)^{\Delta'}$ because $\Delta' = \Delta^c$. Second, ψ is surjective since $c^{-1}Hc = H$. Finally, since $\psi(x^\Delta y^\Delta) = \psi((xy)^\Delta) = (c^{-1}(xy)c)^{\Delta'} = (c^{-1}xc)^{\Delta'}(c^{-1}yc)^{\Delta'} = \psi(x^\Delta)\psi(y^\Delta)$ for all $x, y \in H$, we conclude that ψ is an isomorphism as claimed. It is now easy to verify that λ and ψ define the required permutation isomorphism.

Exercises

1.6.1 If G and H are both subgroups of $Sym(\Omega)$, show that they are permutation isomorphic if and only if they are conjugate in $Sym(\Omega)$.

1.6.2 In Example 1.6.1, show that it is possible that the kernels of the actions of H on Δ and on Δ' are different.

The theorem is stated for the case of a transitive group G, but if G is not transitive then the result can be applied to the restriction of the action of G to each of the orbits of G.

Theorem 1.6A. *Let G be a group acting transitively on a set Ω, and $H \lhd G$. Then:*

(i) *the orbits of H form a system of blocks for G;*

(ii) *if Δ and Δ' are two H-orbits then H^Δ and $H^{\Delta'}$ are permutation isomorphic;*

(iii) *if any point in Ω is fixed by all elements of H, then H lies in the kernel of the action on Ω;*

(iv) *the group H has at most $|G : H|$ orbits, and if the index $|G : H|$ is finite then the number of orbits of H divides $|G : H|$;*

(v) *if G acts primitively on Ω then either H is transitive or H lies in the kernel of the action.*

PROOF. (i) Let Δ be an orbit for H, and put

$$\Sigma := \{\Delta^x \mid x \in G\}.$$

Since H is normal, each Δ^x is an orbit for H (by Exercise 1.4.6), and because G is transitive the union of these orbits is the whole of Ω. Thus every orbit of H appears in Σ, and Σ is a system of blocks for G.

(ii) This follows from (i) and Example 1.6.1.

(iii) If H fixes a point, then it has an orbit of length 1 and so by (i) all of its orbits have length 1; hence H lies in the kernel of the action.

(iv) This follows at once from (i) since all blocks in a system of blocks have the same size.

(v) This also follows at once from (i) since primitivity implies that the blocks must be trivial. □

In reference to (iii) just mentioned, it is useful to introduce the following notation. Suppose that the group G acts on a set Ω and let T be a subset of G. Then we define the *support* and set of *fixed points* of T by

$$\mathrm{supp}(T) := \{\alpha \in \Omega \mid \alpha^x \neq \alpha \quad \text{for at least one } x \in T\}$$

and

$$\mathrm{fix}(T) := \{\alpha \in \Omega \mid \alpha^x = \alpha \quad \text{for all } x \in T\}.$$

In cases where there may be ambiguity we use $\mathrm{supp}_\Omega(T)$ and $\mathrm{fix}_\Omega(T)$ to emphasize the set involved. Note that Ω is the disjoint union of these two sets. The most important cases are when T is a singleton (and we write $\mathrm{supp}(x)$ and $\mathrm{fix}(x)$ in place of $\mathrm{supp}(T)$ and $\mathrm{fix}(T)$), and when T is a subgroup of G. When $\Gamma \subseteq \Omega$, it is often convenient to identify $Sym(\Gamma)$ with the subgroup of $Sym(\Omega)$ consisting of all $x \in Sym(\Omega)$ with $\mathrm{supp}(x) \subseteq \Gamma$.

Exercises

1.6.3 If G acts transitively on Ω and $\alpha \in \Omega$, show that $|N_G(G_\alpha) : G_\alpha| = |\mathrm{fix}(G_\alpha)|$.

1.6.4 Suppose that G is a transitive subgroup of S_n and that $H \leq G$ has k conjugates in G. If $\mathrm{GCD}(k, n) = 1$, show that $N_G(H)$ is transitive and that hence all orbits of H have the same length. [*Hint:* If A and B are subgroups of relatively prime index in a finite group C, then $C = AB = BA$.]

1.6.5 Let G be a transitive subgroup of $Sym(\Omega)$ and let $\alpha \in \Omega$. Show that $\mathrm{fix}(G_\alpha)$ is a block for G. In particular, if G is primitive, then either $\mathrm{fix}(G_\alpha) = \{\alpha\}$ or else $G_\alpha = 1$ and G has finite prime degree.

1.6.6 Let $FSym(\Omega)$ be the set of elements in $Sym(\Omega)$ which have finite support. Show that $FSym(\Omega)$ is a primitive normal subgroup of $Sym(\Omega)$, and is a proper subgroup whenever Ω is infinite. ($FSym(\Omega)$ is called the *finitary symmetric group* on Ω. Of course, $FSym(\Omega) = Sym(\Omega)$ when Ω is finite).

1.6.7 If $x, y \in Sym(\Omega)$ and $\Gamma := \mathrm{supp}(x) \cap \mathrm{supp}(y)$, show that $\mathrm{supp}[x, y] \subseteq \Gamma \cup \Gamma^x \cup \Gamma^y$. In particular, if $|\Gamma| = 1$, show that $[x, y]$ is a 3-cycle. ($[x, y] := x^{-1}y^{-1}xy$ is the commutator of x and y.)

One important normal subgroup in every symmetric group is the *alternating* subgroup $Alt(\Omega)$ (or A_n if $\Omega = \{1, 2, \ldots, n\}$). Indeed as we shall see later, when $n \neq 4$, the only normal subgroups of S_n are $1, A_n$ and S_n. In order to define $Alt(\Omega)$ we first have to define what we mean by odd and even permutations.

Let x be an element of the finitary symmetric group $FSym(\Omega)$ (see Exercise 1.6.6 above). Then x has finite support, and so it has only a finite number of nontrivial cycles of finite length and none of infinite length. Let $m_1, \ldots, m_k$ be the lengths of the nontrivial cycles, and define

$$\lambda(x) := (m_1 - 1) + \ldots + (m_k - 1) = |\mathrm{supp}(x)| - k$$

If $\lambda(x)$ is even we call x an *even* permutation, and if $\lambda(x)$ is odd, we call x an *odd* permutation. When Ω is infinite only permutations with finite support are classified in this way.

Lemma 1.6A. *The mapping $x \mapsto (-1)^{\lambda(x)}$ is a group homomorphism of $FSym(\Omega)$ into the multiplicative group $\{1, -1\}$. It is surjective when $|\Omega| \geq 2$.*

PROOF. From the identities

$$(12\ldots r)(1'2'\ldots s')(11') = (12\ldots r1'2'\ldots s')$$

and

$$(12\ldots r1'2'\ldots s')(11') = (12\ldots r)(1'2'\ldots s')$$

we see that for any $x \in FSym(\Omega)$ and any 2-cycle $(\alpha\beta)$ we have

$$\lambda(x(\alpha\beta)) = \lambda(x) - 1 \text{ or } \lambda(x) + 1$$

depending on whether or not α and β lie in the same cycle of x. (In checking this, note that α or β may possibly lie in 1-cycles of x.)

Since $\lambda(y) = 0$ only when y is the identity element I, we deduce:

(i) there exist 2-cycles $(\alpha_i\beta_i)$ $(i = 1, \ldots, m)$ with $m = \lambda(x)$ such that $x(\alpha_1\beta_1)\ldots(\alpha_m\beta_m) = I$ and so x can be written as a product of $\lambda(x)$ 2-cycles: $(\alpha_m\beta_m)\ldots(\alpha_1\beta_1)$ (which are usually not disjoint);

(ii) if x can be written as a product $(\gamma_1\delta_1)\ldots(\gamma_n\delta_n)$ of n 2-cycles, then $x(\gamma_n\delta_n)\ldots(\gamma_1\delta_1) = I$ and so we have $\lambda(x) = \epsilon_n + \ldots + \epsilon_1 \equiv n \pmod 2$ for some $\epsilon_i = \pm 1$.

These two observations show that every $x \in FSym(\Omega)$ can be written as a product of 2-cycles, and that however this is done the number of 2-cycles required is either always odd or always even, depending on whether $\lambda(x)$ is odd or even. In particular, for all $x, y \in FSym(\Omega)$ we have

$$\lambda(xy) \equiv \lambda(x) + \lambda(y) \pmod 2$$

and so $x \mapsto (-1)^{\lambda(x)}$ is a homomorphism into $\{1, -1\}$ as required. This homomorphism is surjective whenever $FSym(\Omega)$ contains a 2-cycle. □

We define $Alt(\Omega)$ to be the kernel of the homomorphism defined in Lemma 1.6A. Thus $Alt(\Omega) \lhd FSym(\Omega)$ and $Alt(\Omega)$ is a proper subgroup of index 2 in $FSym(\Omega)$ except in the case where $|\Omega| = 1$. In particular, $A_n \lhd S_n$ for all n.

Exercises

1.6.8 Show that $FSym(\Omega)$ can be generated by the set of all 2-cycles in $Sym(\Omega)$ and that $Alt(\Omega)$ can be generated by the set of all 3-cycles.

1.6.9 Show that S_n is generated by the set of $(n - 1)$ 2-cycles: (12), (13), ..., $(1n)$. Give a similar set of $(n - 2)$ 3-cycles which generates A_n.

1.6.10 Consider the action of S_n on the set of all polynomials with integer coefficients in the variables $X_1, \ldots, X_n$ given by

$$f(X_1, \ldots, X_n)^x := f(X_{1'}, \ldots, X_{n'}) \quad \text{when } x = \begin{pmatrix} 1 & \ldots & n \\ 1' & \ldots & n' \end{pmatrix}.$$

Define

$$\Phi(X_1, \ldots, X_n) := \prod_{i<j} (X_i - X_j).$$

Show that that A_n is the stabilizer of the point Φ.

1.6.11 Let G be a finite group of order $2^t m$ where $t \geq 1$ and m is odd. If G contains an element of order 2^t, show that G has a normal subgroup of order m. [*Hint:* First show that the image of the regular representation of G contains a odd permutation, and hence G has a normal subgroup of index 2.]

1.6.12 If G is a primitive subgroup of S_{2m} where m is odd, show that G contains a subgroup of order 4.

In comparing actions (and representations) of a group G, we find that some are "essentially the same" and differ only in the labelling of the points of the sets involved. In other cases the actions are clearly different. For example, the automorphism group A of the trivalent tree $\mathcal{T}$ (Example 1.5.4) acts in a natural way on the set of edges of the tree as well as on the set of vertices, but these actions are distinct since the stabilizer of a vertex has orbits of lengths $1, 3, 6, 12, \ldots$ on the vertices while the stabilizer of an edge has orbits of lengths $1, 4, 8, 16, \ldots$ on the edges. On the other hand, it is not at all clear whether the representations of a group G on the set of left cosets and on the set of right cosets of a subgroup H (see Example 1.3.4 and Exercise 1.3.2) are really different or not.

Let $\rho : G \to Sym(\Omega)$ and $\sigma : G \to Sym(\Gamma)$ be two permutation representations of a group G. These representations are *equivalent* if Ω and Γ have the same cardinality and there is a bijection $\lambda : \Omega \to \Gamma$ such that

$$\lambda(\alpha^{\rho(x)}) = (\lambda(\alpha))^{\sigma(x)} \quad \text{for all } \alpha \in \Omega \text{ and } x \in G.$$

We say that two actions of G are *equivalent* when the corresponding representations are equivalent. This definition should be compared with the definition of permutation isomorphism given above (see Exercise 1.6.17).

In the case that $\Omega = \Gamma$ the bijection λ will be a permutation of Ω and so for some $c \in Sym(\Omega)$ we have $\lambda(\alpha) = \alpha^c$. Thus in this case the two representations are equivalent if and only if for some $c \in Sym(\Omega)$ we have $\sigma(x) = c^{-1}\rho(x)c$ for all $x \in G$.

When the two actions are transitive there is a simple criterion for deciding whether or not they are equivalent.

Lemma 1.6B. *Suppose that the group G acts transitively on the two sets Ω and Γ, and let H be a stabilizer of a point in the first action. Then the*

actions are equivalent $\iff$ *H is the stabilizer of some point in the second action.*

PROOF. Let $\rho : G \to Sym(\Omega)$ and $\sigma : G \to Sym(\Gamma)$ be the representations of G which correspond to the given actions. Then, for some point $\alpha \in \Omega$, the subgroup $H = \{x \in G \mid \alpha^{\rho(x)} = \alpha\}$. If there is an equivalence of the two representations given by a bijection $\lambda : \Omega \to \Gamma$, then $\alpha^{\rho(x)} = \alpha \iff \lambda(\alpha) = \lambda(\alpha^{\rho(x)}) = (\lambda(\alpha))^{\sigma(x)}$, and so H is also the stabilizer of the point $\lambda(\alpha)$ in the second action.

Conversely, suppose that H is also the stabilizer of a point β in the second action, so $x \in H \iff \alpha^{\rho(x)} = \alpha \iff \beta^{\sigma(x)} = \beta$. We claim that we can define a bijection $\lambda : \Omega \to \Gamma$ by

$$\lambda(\alpha^{\rho(x)}) := \beta^{\sigma(x)} \quad \text{for all } x \in G.$$

To do this we first have to show that λ is well-defined, namely, if $\alpha^{\rho(x)} = \alpha^{\rho(y)}$ then the value defined for λ must be the same. This is true because $\alpha^{\rho(x)} = \alpha^{\rho(y)} \iff xy^{-1} \in H \iff \beta^{\sigma(x)} = \beta^{\sigma(y)}$. Second, λ is defined for all points in Ω because the representation ρ is transitive, and similarly λ is surjective because σ is transitive. Finally, λ is injective because $\alpha^{\rho(x)} = \alpha^{\rho(y)} \iff \beta^{\sigma(x)} = \beta^{\sigma(y)}$; and so λ is a bijection from Ω onto Γ. Now for each $\gamma \in \Omega$ there exists $a \in G$ such that $\gamma = \alpha^{\rho(a)}$, and so for each $x \in G$ we have

$$\lambda(\gamma^{\rho(x)}) = \lambda(\alpha^{\rho(ax)}) = \beta^{\sigma(ax)} = (\beta^{\sigma(a)})^{\sigma(x)} = (\lambda(\alpha^{\rho(x)}))^{\sigma(x)} = \lambda(\gamma)^{\sigma(x)}$$

which proves that the two representations are equivalent. □

Lemma 1.6B enables us — at least in theory — to describe up to equivalence all transitive permutation representations of a given group G. Indeed, if H is a subgroup of G, then Example 1.3.4 shows that the action of G on the set Γ_H of right cosets of H gives a representation ρ_H of G in which the point stabilizers are just the conjugates of H in G ($x^{-1}Hx$ is the stabilizer of the point $Hx \in \Gamma_H$). Thus Lemma 1.6A shows that every transitive representation of G is equivalent to ρ_H for some $H \leq G$, and that ρ_H and ρ_K are equivalent exactly when H and K are conjugate in G. Hence the transitive representations of G are given up to equivalence by the representations ρ_H as H runs over a set of representatives of the conjugacy classes of subgroups of G.

EXAMPLE 1.6.2. Let $G = S_3$. Then a complete set of representatives of the conjugacy classes of subgroups of G is given by: $1, \langle(12)\rangle, \langle(123)\rangle$ and S_3. These give transitive representations of G of degrees 6,3,2 and 1, respectively, where the first two are faithful. This shows, for example, that if S_3 acts faithfully on a set of size 8 then it must have either an orbit of size 6, or one or two orbits of size 3, and the remaining orbits are of sizes 1 or 2.

Exercises

1.6.13 Show that if H is a subgroup of a group G, then the action of G on the set of right cosets of H and the action of G on the set of left cosets of H (see Exercise 1.3.2) are equivalent.

1.6.14 The group of symmetries of the cube acts on the set of 12 edges of the cube and on the set of 12 diagonals in the faces of the cube. Are these two actions equivalent?

1.6.15 Find up to equivalence all the transitive representations of S_4.

1.6.16 Let G be a group acting on a set Ω, and let $\alpha \in G$. Suppose that K is a transitive normal subgroup K of G and that $K_\alpha = 1$. Show that the action of G_α on Ω and the action of G_α on K by conjugation (Example 1.3.5) are equivalent.

1.6.17 Show that S_6 has two inequivalent transitive representations of degree 6 but the images of the representations are permutation isomorphic.

An intransitive group $G \le Sym(\Omega)$ may have different actions on different orbits and the groups induced on these orbits may be interrelated in intricate ways. In certain situations, however, we can reconstruct G in a simple way, from the groups G induces on its orbits on Ω.

Recall that when $\Delta \subseteq \Omega$ we may identify $Sym(\Delta)$ with the subgroup of $Sym(\Omega)$ consisting of the elements whose support lies in Δ. If $\{\Delta_1, \dots, \Delta_m\}$ is a partition of Ω, and each Δ_i is G-invariant for some $G \le Sym(\Omega)$, then this identification enables us to write $x = x^{\Delta_1} \cdots x^{\Delta_m}$ for all $x \in G$. Thus $G \le G^{\Delta_1} \cdots G^{\Delta_m} = G^{\Delta_1} \times \cdots \times G^{\Delta_m}$. The following theorem gives a useful criterion for equality to hold when $m = 2$.

Theorem 1.6C. *Suppose that $G \le Sym(\Omega)$ and that $\Delta \ne \emptyset, \Omega$ is a G-invariant subset of Ω. Put $\Gamma := \Omega \setminus \Delta$. If G^Δ and G^Γ have no nontrivial homomorphic image in common then $G = G^\Delta \times G^\Gamma$.*

PROOF. The homomorphism $x \mapsto x^\Delta$ of G into $Sym(\Delta)$ has kernel $H_1 := G_{(\Delta)}$ and image $H := G^\Delta$. Similarly, $x \mapsto x^\Gamma$ has kernel $K_1 := G_{(\Gamma)}$ and image $K := G^\Gamma$. Since $H \cong G/H_1$ and $K \cong G/K_1$ have the common homomorphic image G/H_1K_1, the hypothesis implies that $G = H_1K_1$. But then $H = G^\Delta = (H_1K_1)^\Delta = K_1$ and $K = G^\Gamma = (H_1K_1)^\Gamma = H_1$. Therefore $G = HK = H \times K$ as asserted. □

Exercises

1.6.18 Suppose that the group G acts transitively on two sets Γ and Δ of size n. Show that these actions are equivalent if and only if G has an orbit of length n in its induced action on $\Gamma \times \Delta$.

1.6.19 Show that no transitive subgroup of S_5 has an elementary abelian 2-group as a point stabilizer.

1.6.20 Let $A = [\alpha(i,j)]$ be an invertible $n \times n$ matrix over a field, and suppose that group G has two actions ρ and σ on the set $\{1, 2, \ldots, n\}$ such that for each $x \in G : \alpha(i^{\rho(x)}, j^{\sigma(x)}) = \alpha(i,j)$ for all i, j. Show that the two actions have the same number of orbits. If G is cyclic, show that they also have the same number of fixed points. However, show that in general the two actions are not equivalent.

1.6.21 Show that every transitive group of degree p^2 (p prime) contains a regular subgroup.

1.7 Orbits and Fixed Points

There is a simple relationship between the number of orbits of a finite group acting on a finite set and the number of fixed points of its elements. A wide range of applications in counting problems and combinatorics is based on elaborations of this relationship. The theorem itself has a long history and is often referred to (inaccurately) as the "Burnside Lemma"; the simplest version is the following result.

Theorem 1.7A (Cauchy–Frobenius Lemma). *Let G be a finite group acting on a finite set Ω. Then G has m orbits on Ω where*

$$m\,|G| = \sum_{x \in G} |\mathrm{fix}(x)|\,.$$

Proof. Consider the set $\mathcal{F} = \{(\alpha, x) \in \Omega \times G \mid \alpha^x = \alpha\}$; we shall count the number of elements of $\mathcal{F}$ in two ways. First, suppose that the orbits of G are $\Omega_1, \ldots, \Omega_m$. Then, using the orbit-stabilizer property, we have

$$|\mathcal{F}| = \sum_{i=1}^{m} \sum_{\alpha \in \Omega_i} |G_\alpha| = \sum_{i=1}^{m} \sum_{\alpha \in \Omega_i} \frac{|G|}{|\Omega_i|} = \sum_{i=1}^{m} |G| = m\,|G|\,.$$

Second,

$$|\mathcal{F}| = \sum_{x \in G} |\mathrm{fix}(x)|.$$

The result follows. □

Since $|\mathrm{fix}(x)|$ remains constant on each conjugacy class of G, the relation in Theorem 1.7A can be rewritten as

$$m\,|G| = \sum_{i=1}^{k} |C_i|\,|\mathrm{fix}(x_i)|$$

where $C_1, C_2, \ldots, C_k$ are the conjugacy classes of G and x_i is a representative of C_i. This form is often simpler in calculations.

Exercises

1.7.1 If G is a transitive subgroup of S_n show that

$$\sum_{x \in G} |\text{fix}(x)| = |G| \quad \text{and} \quad \sum_{x \in G} |\text{fix}(x)|^2 = r\,|G|$$

when the point stabilizers of G have r orbits.

1.7.2 If G is a transitive subgroup of S_n, show that G has at least $n-1$ elements each of which fixes no point. Conclude that if G is any finite group, and H is a subgroup of index n in G, then G has at least $n-1$ elements which are not conjugate to elements in H.

1.7.3 Give an example of a transitive permutation group of infinite degree in which every element has infinitely many fixed points.

1.7.4 Show that the average number of k-cycles for an element in S_n is equal to $1/k$.

1.7.5 Suppose that G is a finite group with k conjugacy classes. Show that the number of ordered pairs (x, y) of elements from G such that $xy = yx$ is equal to $k\,|G|$. [*Hint:* Let G act on itself by conjugation.]

1.7.6 Let C denote a conjugacy class on a finite group G. If G acts transitively on Ω, show that $|\text{fix}(x)|\,|C| = |G_\alpha \cap C|\,|\Omega|$ for all $\alpha \in \Omega$, $x \in C$.

A common instance of Theorem 1.7A arises when Ω is a set of functions and the group acts on one or both of the underlying sets. Let Γ and Δ be two finite nonempty sets, and let $\Omega := \text{Fun}(\Delta, \Gamma)$ be the set of all functions of Δ into Γ. We may think of the elements of Γ as colours and each function ϕ in $\text{Fun}(\Delta, \Gamma)$ as a colouring of the points of Δ; specifically, ϕ colours the point α with colour $\phi(\alpha)$.

For example, consider the case where Δ is the set of six faces of a cube and $\Gamma = \{\text{red, white, blue}\}$. Then $\text{Fun}(\Delta, \Gamma)$ represents the set of all colourings of the faces of the cube by the three colours. Two such colourings may be considered *indistinguishable* if the cube with one of these colourings can be mapped into the cube with the other colouring via a rotation of the cube; this is equivalent to saying that the two colourings lie in the same orbit of $\text{Fun}(\Delta, \Gamma)$ under the action of the group of rotations on Δ. In general, whenever a group G acts on the set Δ, then G has a corresponding action on $\text{Fun}(\Delta, \Gamma)$ with ϕ^x defined by $\phi^x(\alpha) := \phi(\alpha^{x^{-1}})$ for all $\phi \in \text{Fun}(\Delta, \Gamma)$, $x \in G$ and $\alpha \in \Delta$. We shall see this action again in Sect. 2.6 when we discuss wreath products.

Exercise

1.7.7 Show that the definition of ϕ^x just given does define an action of G on $\text{Fun}(\Delta, \Gamma)$ and explain why x^{-1} rather than x must be introduced on the right hand side.

The proof of the following result is left as an exercise (Exercise 1.7.8).

Corollary 1.7A. *Let Δ and Γ be finite nonempty sets and let G be a finite group acting on Δ. For each $x \in G$, let $c(x)$ denote the number of cycles (including cycles of length 1) which x has in its action on Δ. Then the number of orbits of G acting on Fun(Δ, Γ) is*

$$\frac{1}{|G|} \sum_{x \in G} |\Gamma|^{c(x)} .$$

EXAMPLE 1.7.1. (Counting Unlabeled Graphs.) How many graphs are there with n vertices and a single edge? If the vertices are distinguishable, or *labeled*, there are $\binom{n}{2}$ choices for the position of the edge giving $\binom{n}{2}$ distinct graphs. If, on the other hand, the vertices are indistinguishable or *unlabeled* then there is only one such graph, an edge and $n - 2$ isolated vertices. This distinction between labeled and unlabeled graphs has a dramatic impact on the complexity of counting the graphs on n vertices.

A graph on a set Δ of n vertices is completely determined by its set Σ of edges where an edge is a subset of size 2 from Δ. Since Δ has $\binom{n}{2}$ subsets of size 2, there are $2^{\binom{n}{2}}$ possible choices for Σ; this gives the number of labeled graphs on n vertices. The corresponding problem of counting the unlabeled graphs on n vertices is more subtle.

Let $\Delta^{\{2\}}$ denote the set of all subsets of size 2 from Δ and let $\Gamma := \{0, 1\}$. Then the set of labeled graphs on the vertex set Δ may be identified with the set Fun$(\Delta^{\{2\}}, \Gamma)$ where $\phi \in$ Fun$(\Delta^{\{2\}}, \Gamma)$ corresponds to the graph whose set of edges consists of the elements of $\Delta^{\{2\}}$ which ϕ maps onto 1. The symmetric group $G := Sym(\Delta)$ acts on $\Delta^{\{2\}}$ in a natural way and hence acts on Fun$(\Delta^{\{2\}}, \Gamma)$ as described above. Two graphs on Δ are indistinguishable as unlabeled graphs precisely when the corresponding functions lie in the same orbit of G. Thus, if we take $\Delta = \{1, 2, \ldots, n\}$, then Corollary 1.7A shows that the number of unlabeled graphs on n vertices is precisely

$$\frac{1}{n!} \sum_{x \in Sym(\Delta)} 2^{c(x)}$$

where $c(x)$ is the number of cycles of x acting on $\Delta^{\{2\}}$.

Exercises

1.7.8 Prove Corollary 1.7A.

1.7.9 State and prove the corresponding theorem when, as well as the group G acting on Δ, we have a group H acting on the set Γ making some sets of colours indistinguishable. (For example, in cases where we are only interested in using the mapping ϕ to partition Δ, but do not wish to label the partitions, H will be the full symmetric group $Sym(\Gamma)$).

1.7.10 Show that $k(k^2 + 1)(k^2 + 4)/10$ indistinguishable circular necklaces can be made from five beads if beads of k different colours are available. Assume that two necklaces are indistinguishable if one can be obtained from the other using a cyclic permutation or a flip. Generalize to the case of necklaces with n beads.

1.7.11 Declare two colourings of a cube to be indistinguishable if one can be obtained from the other by a rotation of the cube. How may indistinguishable ways are there to colour a cube in k colours? What is the answer to the corresponding problem if we permit arbitrary symmetries (including reflections) of the cube?

1.7.12 Let G be a finite group acting on a finite nonempty set Ω, and suppose that G has m orbits: $\Omega_1, \Omega_2, \dots, \Omega_m$. The following algorithm can be used to select a random element α from Ω in such a way that the probability that α lies in Ω_i is $1/m$ (independent of the orbit). For example, it can be used to choose an unlabeled graph uniformly at random from the set of all unlabeled graphs on n vertices.

Step 0: For each conjugacy class C of G, pick an element x_C, and compute

$$p(C) := \frac{|C|\,|\text{fix}(x_C)|}{m\,|G|}.$$

Since $\sum p(C) = 1$ by Theorem 1.7A, this gives a probability distribution defined on the set of conjugacy classes of G. Clearly $p(C)$ is independent of the choice of x_C, and $p(C) = 0$ if elements of C have no fixed points.

Step 1: Choose a conjugacy class C according to the probability distribution given by Step 0.

Step 2: Choose α uniformly at random from $\text{fix}(x_C)$.

Show that, for each orbit Ω_i of G, the probability that α lies in Ω_i is equal to $1/m$.

1.7.13 Let G be a finite group acting on a set Ω of size n, and let $f : G \to \mathbb{C}$ be a class function (that is, $f(x) = f(y)$ whenever x and y lie in the same conjugacy class of G). Show that for each $\alpha \in \Omega$ we have:

$$\sum_{x \in G} f(x)\,|\text{fix}(x)| = n \sum_{y \in G_\alpha} f(y).$$

(Since $|\text{fix}(x)|$ and the constant functions are class functions this exercise generalizes Exercise 1.7.1.)

1.7.14 Let G be a finite transitive group of order g and degree n. Suppose the point stabilizers of G have r orbits. Show that the number of elements of G which fix at least one point lies between g/r and $(n - r)g/(n - 1) + 1$.

1.8 Some Examples from the Early History of Permutation Groups

The original development of groups began with the study of permutation groups, and even before that permutations had arisen in work of Lagrange in 1770 on the algebraic solution of polynomial equations. By the middle of the 19th century there was a well-developed theory of groups of permutations due in a large part to Camille Jordan and his book "Traité des Substitutions et des Équations Algébriques"(1870) which in turn was based on the papers left by Évariste Galois in 1832. Again, the primary motivation of Jordan was what is now called "Galois theory".

The classical problem in the algebraic study of polynomial equations was to determine the roots of a polynomial in terms of an algebraic formula involving the coefficients. Early mathematicians sought a formula or algorithm which constructed these roots explicitly using rational operations (addition, subtraction, multiplication and division) and extraction of kth roots. The paradigm for this "solution by radicals" was the familiar formula for quadratic equations which had been known to the Babylonians, and by the end of the 16th century similar formulae had been derived for cubic and quartic equations. Joseph Louis Lagrange in his 1770 paper also showed how particular polynomials of higher degree had solutions by radicals, but the question of whether all polynomials of the 5th degree had solutions of this form remained open until the beginning of the 19th century. At that point it was shown by Paolo Ruffini in 1802 and Niels Abel in 1826 that no such general solution could be found. The final achievement of this period was due to Galois who associated a permutation group to each polynomial and showed that the structure of the group indicated whether or not the polynomial could be solved by radicals.

Galois' results were based on Lagrange's 1770 paper. In that paper Lagrange had made a thorough analysis of the known algorithms for solving polynomials of degree up to 4, and showed how they relied in various ways on finding "resolvent" polynomials. These latter polynomials can be constructed effectively from the original polynomials and have the property that the roots of the original polynomials can be determined from the roots of the resolvent. To be useful, the resolvent must either be easy to solve itself, or be amenable to further reduction. In the case of cubic and quartic polynomials the resolvents are of degrees 2 and 3, respectively, but Lagrange noted that, for polynomials of degree greater than 4, the degrees of the resolvents are larger than the degrees of the original polynomials. The process of constructing resolvents described below is essentially the method using permutations which Lagrange introduced.

Consider a set of n variables $\{X_1, \ldots, X_n\}$. The symmetric group S_n acts on this set by permuting the subscripts, and we can extend this action of S_n to an action on the set of polynomials in the variables in a natural

way. For example, if $z = (12)(34) \in S_4$ and $\Phi = X_1X_3 - X_2X_4$, then $\Phi^z = X_2X_4 - X_1X_3 = -\Phi$. The orbit of Φ under the full symmetric group S_4 consists of the six polynomials:

$$\pm(X_1X_3 - X_2X_4),\ \pm(X_1X_2 - X_3X_4),\ \pm(X_1X_4 - X_2X_3).$$

Lagrange referred to these six polynomials as the *values* of Φ. The orbit-stabilizer property tells us that the stabilizer of Φ in S_4 has order 4.

Exercises

1.8.1 Find the "values" of the following polynomials in $X_1, \ldots, X_5$:
 (i) $X_1 + X_2 + X_3 + X_4 + X_5$;
 (ii) X_1;
 (iii) $X_1 + 2X_2 + 3X_3 + 4X_4 + 5X_5$;
 (iv) $\prod_{i<j}(X_i - X_j)$;
 (v) $X_1 + X_2 + 3X_3 + 4X_4 + 5X_5$.

1.8.2 Show that no polynomial in 5 variables has exactly 3, 4 or 8 values.

In general, let Φ be a polynomial in $X_1, \ldots, X_n$ with k values, $\Phi^{(1)} = \Phi, \ldots, \Phi^{(k)}$. Then the *resolvent* is a polynomial in $X_1, \ldots, X_n$ and Z given by

$$h(Z) := \prod_{i=1}^{k}(Z - \Phi^{(i)}) = \sum_{j=0}^{k} h_j(X_1, \ldots, X_n)Z^j.$$

Since the $\Phi^{(i)}$ form an orbit under S_n, the polynomial h is invariant under an arbitrary permutation of $X_1, \ldots, X_n$. Thus each polynomial $h_j(X_1, \ldots, X_n)$ is symmetric in $X_1, \ldots, X_n$ and so can be written as a polynomial in the elementary symmetric functions of these variables (the "symmetric function theorem"). If $f(X)$ is a polynomial of degree n with roots $r_1, \ldots, r_n$, then the elementary symmetric functions of these roots can be expressed in simple terms in the coefficients of $f(X)$. Hence, if we substitute $r_1, \ldots, r_n$ for $X_1, \ldots, X_n$ in the expression for $h(Z)$ we obtain a polynomial in Z whose coefficients can be effectively calculated from the coefficients of $f(X)$. Moreover, if Φ has been chosen carefully, then it may happen that we can solve the polynomial $h(Z)$ and be able to compute the roots $r_1, \ldots, r_n$ from the roots $\Phi^{(1)}(r_1, \ldots, r_n), \ldots, \Phi^{(k)}(r_1, \ldots, r_n)$ of $h(Z)$.

It was using these methods of resolvents that Ruffini and Abel were able to give proofs that there is no solution by radicals for equations of degree greater than 4 (Ruffini's proof was not complete). The subsidiary problem of determining what number of values were possible for suitable polynomials of n variables, and finding such polynomials, continued to play an important role in the development of permutation groups in the 19th century.

Exercises

1.8.3 If n is a multiple of an odd prime p, show that a polynomial in n variables has at least p values.

1.8.4 (Solution of the cubic) Let $f(X)$ be a real cubic polynomial with roots r_1, r_2, r_3, and consider the polynomial

$$\Phi = (X_1 + \omega X_2 + \omega^2 X_3)^3$$

where ω is a complex cube root of 1 with $\omega \neq 1$. Show:

(i) Φ lies in an orbit of length 2 under S_3, say $\{\Phi, \Phi^*\}$; and

(ii) the roots of $f(X)$ can be calculated from the coefficients of $f(X)$ and the numbers $\Phi(r_1, r_2, r_3)$ and $\Phi^*(r_1, r_2, r_3)$ using rational operations and extraction of cube roots.

After the work of Ruffini and Abel there remained the question of deciding whether a particular polynomial could be solved using radicals. This problem was solved — at least in principal — by Galois in 1830. To each polynomial $f(X)$ with distinct roots $r_1, \ldots, r_n$ Galois associated a permutation group on the set of roots (now called the "Galois group" of $f(X)$), and the structure of this group determines whether or not $f(X)$ can be solved by radicals. In modern terms we begin with a field K containing the coefficients of $f(X)$ and adjoin the roots to obtain a splitting field L. The field automorphisms of L which fix every element of K form a finite group G which acts on the set of roots. The permutations of $\{r_1, \ldots, r_n\}$ induced by the elements of G constitute the *Galois group* of $f(X)$. Of course Galois worked without the language of fields and automorphisms so his original definition has quite a different ring to it.

The relation between the Galois group and the Lagrange resolvent is as follows. Suppose we can find a polynomial Φ over K such that each of the roots r_i can be written as a polynomial (over K) in $t := \Phi(r_1, \ldots, r_n)$. In modern terms this means that $K(r_1, \ldots, r_n) = K(t)$. Then for each $x \in S_n$ we define $t^x := \Phi(r_{1'}, \ldots r_{n'})$ where $\imath' := \imath^x$ for each i. We can then construct the resolvent (a polynomial of degree $n!$ over K):

$$g(Z) := \prod_{x \in S_n} (Z - t^x).$$

Now factor $g(Z)$ over K and determine an irreducible factor $g_1(Z)$ which has t as a root. Suppose that G is the Galois group for $f(X)$. Then $g_1(Z)$ has degree $|G|$, and the roots of $g_1(Z)$ are precisely t^x for $x \in G$.

It is interesting to note that permutations were used in the study of algebraic equations long before there was a clear definition of a group. The point is that the basic concepts of transitivity, primitivity and closure under conjugation are meaningful for sets of permutations whether or not these sets are closed under multiplication.

Many of the basic concepts introduced in this chapter can be traced back to work of Augustin-Louis Cauchy in the first half of the 19th century.

Galois' work remained unread for many years after his tragic death in 1832 at the age of 21. His seminal papers were eventually published by Joseph Liouville in 1846, and then in the 1860s Jordan wrote his influential book which developed Galois' ideas on permutation groups and fields in a form which was easily available to his contemporaries. At that point there was a clear concept of permutation group, a well-developed theory, a rich and growing supply of examples, and applications of the theory in a number of different branches of mathematics. Jordan's name will appear frequently in the chapters which follow.

1.9 Notes

Many books on general group theory contain useful sections dealing with basic results from permutation groups, or chapters on special topics in this area. Books which we have found useful include: Biggs and White (1979), Burnside (1911), Carmichael (1937), Hall (1957), Huppert (1967), W.R. Scott (1964), and Tsuzuku (1982). In addition, there are more specialized texts which deal with specific topics in permutation groups such as: Cameron (1990), Huppert and Blackburn (1982b), Neumann et al. (1994), Passman (1968) and Wielandt (1964). We shall refer to these later.

The earliest text on permutation groups is C. Jordan's *Traité de substitutions et des équations algébraiques* [Jordan (1870)] which was reprinted in 1957 and so is available in many libraries. Another classical book of more than historic interest, with several chapters on permutation groups, is Burnside (1911); this has also been reprinted. With a few notable exceptions, group theory was largely ignored during much of the first half of this century (Burnside's contributions to group theory are hardly mentioned in his mathematical obituary), but interest was rejuvenated in the 1950s. The Wielandt book (1964) (originally appearing as a set of notes in German in 1955) presented classical results on finite permutation groups in modern language as well as Wielandt's own work. This book has since remained the standard reference to finite permutation groups; notation introduced by Wielandt is now commonly used, and the book has strongly influenced the development of the area. Later lecture notes by Wielandt on infinite permutation groups [Wielandt (1960b)], permutation groups and invariant relations [Wielandt (1969)] and permutation groups and subnormal subgroups [Wielandt (1971a) and (1971b)] circulated informally, but were not so widely available. Fortunately, these lecture notes have now been reprinted in Wielandt (1994).

The material of Chapter 1 is classical, with the exception of some of the exercises.

- Exercise 1.2.16: There is an extensive literature on the "pancake flipping problem". See, for example, Gates and Papadimitriou (1979).

- Sect. 1.3 The problem of faithful representations is discussed in Easdown and Praeger (1988).
- Exercise 1.3.6: See Zagier (1990).
- Exercise 1.4.11: See Wielandt (1959).
- Exercise 1.4.18: See Shalev (1994).
- Exercises 1.5.20–21: See Sheppard and Wiegold (1963), Neumann and Vaughan–Lee (1977) and Kovacs and Newman (1988) for related work.
- Exercise 1.6.20: See Brauer (1941).
- Theorem 1.7A: The provenance of this result is discussed in Neumann (1979). Expositions of the generalized version introduced in Pólya (1937) appear in many books on combinatorics. See also Foulkes (1963), Read (1968), and Kerber (1986).
- Exercise 1.7.2: Using the classification of finite simple groups, it has been shown that each nontrivial finite transitive group contains a fixed point free element of prime power order [see Fein et al (1981)].
- Exercise 1.7.12: See Dixon and Wilf (1983).
- Exercise 1.7.14: See Cameron and Cohen (1992).

2

Examples and Constructions

In order to understand the development of a subject it is helpful to have available a wide range of examples. The aim of the present chapter is to provide such examples and to give some general constructions of permutation groups which we shall use in later chapters.

2.1 Actions on k-tuples and Subsets

We begin with some easy constructions which allow us to generate new examples of group actions from old ones. Let G be a group acting on a set Ω, and let Ω^k ($k \geq 1$) denote the k-th cartesian power of Ω. Then G acts on Ω^k in a natural way, namely: $(\alpha_1, \dots, \alpha_k)^x := (\alpha_1^x, \dots, \alpha_k^x)$ for all $x \in G$. Moreover, the subset of Ω^k consisting of k-tuples of *distinct* points is clearly G-invariant for every choice of G and k; we shall denote this subset by $\Omega^{(k)}$. Note that when Ω is finite with $|\Omega| = n$, we have $\left|\Omega^{(k)}\right| = n!/(n-k)!$.

EXAMPLE 2.1.1. Consider the action of S_4 on $\Omega^{(2)}$ where $\Omega := \{1, 2, 3, 4\}$. This action has degree $4!/2! = 12$. In the corresponding representation the only nontrivial elements of S_4 which fix a point in $\Omega^{(2)}$ are the 2-cycles. For example, using the notation $\alpha\beta$ to denote an element $(\alpha, \beta) \in \Omega^{(2)}$ we have

$$(1\ 2) \mapsto (12, 21)(13, 23)(31, 32)(14, 24)(41, 42).$$

If G is a group acting on a set Ω and k is an integer with $1 \leq k \leq |\Omega|$, then we say G is *k-transitive* if G is transitive on $\Omega^{(k)}$. We say that G is *highly transitive* if Ω is infinite and G is k-transitive for all integers $k \geq 1$.

Exercises

2.1.1 If G is a group acting on Ω, show that G is transitive if and only if G is 1-transitive. Moreover, if $k > 1$, show that G is $(k-1)$-transitive whenever G is k-transitive.

2.1.2 If G is a finite k-transitive group of degree n, show that $|G|$ is divisible by $n(n-1)\dots(n-k+1)$.
2.1.3 Show that G acts k-transitively on Ω (where $k \leq |\Omega|$) $\iff$ G is $(k-1)$-transitive and, for any $(k-1)$-subset $\Delta \subseteq \Omega$, the group $G_{(\Delta)}$ acts transitively on $\Omega \setminus \Delta$.
2.1.4 Show that $Sym(\Omega)$ is k-transitive for all positive integers $k \leq |\Omega|$. If $G \leq S_n$, show that G is $(n-2)$-transitive $\iff$ $A_n \leq G$.
2.1.5 Show that $Alt(\Omega)$ is highly transitive whenever Ω is infinite.
2.1.6 Suppose G is k-transitive for some $k \geq 2$, and N is a nontrivial normal subgroup of G. Show that N is $(k-1)$-transitive. In particular, if G is highly transitive, then so is N.

It is interesting to observe that finite multiply transitive groups arose very early in the history of permutation groups. In particular, Évariste Galois constructed a family of 3-transitive groups in 1830 (see Sect. 2.8). In 1861–1873 Émile Mathieu discovered a series of multiply transitive groups which are now named after him, including 5-transitive groups of degrees 12 and 24; we shall describe these in Chap. 6. Mathieu's remarkable groups are now known to be quite exceptional, and their discovery led to what has turned out to be a dead-end in permutation groups — the study of finite multiply transitive groups of high transitivity. In fact the classification of finite simple groups shows that except for the Mathieu groups (and the trivial examples of A_n and S_n) no finite permutation groups are more than 3-transitive. We shall not prove this, but we shall prove some slightly weaker results in the chapters to follow. For an infinite class of finite 3-transitive groups see Sect. 2.8. In contrast to the finite case there seems to be a rich class of highly transitive groups of infinite degree. See Chap. 7 for more details on multiply transitive groups and Chap. 9 for further infinite examples.

A second kind of easily constructed action of G is its action on the set of all subsets of Ω via $\Gamma^x := \{\gamma^x \mid \gamma \in \Gamma\}$ for each $\Gamma \subseteq \Omega$ and $x \in G$. Again it is easy to see that all subsets of a given size constitute a G-invariant set in this action. We shall use the notation $\Omega^{\{k\}}$ to denote the set of all *k-subsets* (that is, subsets of size k) of Ω for $k = 1, 2, \dots$. If Ω is finite of size n, then $\left|\Omega^{\{k\}}\right| = \binom{n}{k}$ for $1 \leq k \leq n$. A group G acting on a set Ω is called *k-homogeneous* if it is transitive on the set $\Omega^{\{k\}}$ $(1 \leq k \leq |\Omega|)$. We call G *highly homogeneous* if Ω is infinite and G is k-homogeneous for each integer $k \geq 1$. A few results on k-homogeneous groups are presented here; a more complete discussion is deferred to Sect. 9.5.

Clearly k-transitive implies k-homogeneous; we can be a little more precise. If $\Delta = \{\delta_1, \dots, \delta_k\}$ is a k-subset of Ω, then the stabilizer of the "point" Δ in the action of G on $\Omega^{\{k\}}$ is the setwise stabilizer $G_{\{\Delta\}}$. The pointwise stabilizer $G_{(\Delta)}$ is the stabilizer of the "point" $(\delta_1, \dots, \delta_k)$ in the action of G on $\Omega^{(k)}$. As we saw in Sect. 1.6, the representation of $G_{\{\Delta\}}$ associated with its action on Δ defines a homomorphism $x \mapsto x^\Delta$ of $G_{\{\Delta\}}$

into $Sym(\Delta) \cong S_k$ with kernel $G_{(\Delta)}$, and so the factor group $G_{\{\Delta\}}/G_{(\Delta)}$ is isomorphic to a subgroup of S_k. See Sect. 9.5 for further discussion of homogeneous groups.

EXAMPLE 2.1.2. Consider the action of S_n on $\Omega^{\{2\}}$ where $\Omega := \{1, 2, \ldots, n\}$ and $n \geq 3$. Since S_n is n-transitive on Ω, this action is transitive. Consider the stabilizer H in S_n of the subset $\{1,2\} \in \Omega^{\{2\}}$. The group H has 3 orbits consisting of $\{1,2\}$; $\{1,\alpha\}, \{2,\alpha\}$ for all $\alpha \neq 1,2$; and $\{\alpha,\beta\}$ for all $\alpha,\beta \neq 1,2$. These orbits have lengths $1, 2(n-2)$ and $(n-2)(n-3)/2$, respectively. Now any nontrivial block for the action of S_n on $\Omega^{\{2\}}$ which contains the point $\{1,2\}$ must also contain one of the other orbits of H (see Exercise 1.5.9). However, a simple argument shows that for $n \neq 4$ such a block must also contain the other orbit (see Exercise 2.1.8), and so the action of S_n on $\Omega^{\{2\}}$ is primitive. By the orbit-stabilizer property, H is a subgroup of index $n(n-1)/2$ in S_n and H is maximal by Corollary 1.5A.

Exercises

2.1.7 In the example above show that $2(n-2)+1 \leq (n-2)(n-3)/2$ for $n \geq 8$, and that the left hand side never divides the right hand side in this range. Deduce that, except in the case $n = 4$, any block which contains two of the orbits of H must also contain the third. Hence show G acts primitively on $\Omega^{\{2\}}$ for all $n \geq 3$ except $n = 4$.

2.1.8 For which values of n is the action of S_n on $\Omega^{\{3\}}$ primitive?

2.1.9 If G acts on a set Ω of size n, show that G is k-homogeneous $\iff$ G is $(n-k)$-homogeneous.

2.1.10 Show that if G is a 2-homogeneous group of degree > 2 then G is primitive. Give an example where G is not 2-transitive.

2.1.11 Suppose that G is a 2-homogeneous subgroup of S_n with $n \geq 3$. Show that a point stabilizer of G has at most three orbits, and that G is 2-transitive if G has even order.

2.2 Automorphism Groups of Algebraic Structures

Permutation groups frequently arise "in nature" as groups of permutations of various kinds of mathematical objects which preserve the underlying structure of the object in a suitable sense. We mentioned some geometrical examples in Chap. 1, and now turn to some classes of algebraic structures.

EXAMPLE 2.2.1. (Automorphisms of common algebraic structures). Let G be a group and consider the set of all permutations x of G which preserve the group operation in the sense that

$$(ab)^x = a^x b^x \quad \text{for all } a, b \in G$$

(the product of the images equals the image of the product). This set is obviously a subgroup of $Sym(G)$ and is denoted by $\mathrm{Aut}(G)$; its elements are called *automorphisms* (or more specifically *group automorphisms*) of G. Similarly, if V is a vector space over some field F, then the automorphisms of V are the permutations x of V which preserve the vector space operations on V in the sense that

$$(u+v)^x = u^x + v^x \quad \text{and} \quad (\lambda u)^x = \lambda u^x$$

for all $u, v \in V$, and $\lambda \in F$. In this case the term "invertible linear transformation" is commonly used in place of "automorphism" and the group $\mathrm{Aut}(V)$ of all automorphisms is usually denoted by $GL(V)$, the *general linear group* on V. Another example of this type is the automorphism group of a ring R with unity 1; this consists of all permutations x of R which preserve both addition and multiplication in R and also map the distinguished element 1 onto itself:

$$(a+b)^x = a^x + b^x, \ (ab)^x = a^x b^x \quad \text{and} \quad 1^x = 1$$

for all $a, b \in R$. In general, when a group acts on an algebraic structure, we shall say that the action *preserves* the structure if the elements of the group act as automorphisms.

EXAMPLE 2.2.2. Let K be a normal subgroup of the group G and consider the conjugation action of G on K given by $u^x := x^{-1}ux$ $(u \in K, x \in G)$; the kernel is the centralizer $C_G(K)$. This action preserves the group structure of K, and so the image of the corresponding representation lies in $\mathrm{Aut}(K)$. Hence by the "first isomorphism theorem" $G/C_G(K)$ is isomorphic to a subgroup of $\mathrm{Aut}(K)$. In the particular case where $K = G$ then $C_G(G) = Z(G)$, the centre of G, and the automorphisms induced by conjugation by elements of G are called *inner automorphisms*. Thus the group $\mathrm{Inn}(G)$ of inner automorphisms of G is isomorphic to $G/Z(G)$.

Exercises

2.2.1 If a group G acts on an algebraic structure A (such as a group, vector space or a ring) so as to preserve the structure, and T is any subset of G, show that $\mathrm{fix}(T)$ is a substructure of A (such as a subgroup, subspace or subring).

2.2.2 If $\langle x \rangle$ is a finite cyclic group of order n show that

$$\mathrm{Aut}(\langle x \rangle) = \{\sigma_k \mid 1 \le k \le n \text{ and } \mathrm{GCD}(k,n) = 1\}$$

where $\sigma_k : x^i \mapsto x^{ki}$ for each i. What is the automorphism group in the case that $\langle x \rangle$ is infinite? [Note: $\mathrm{GCD}(k,n)$ denotes the greatest common divisor of k and n.]

2.2.3 Let $R := \mathbb{Z}/n\mathbb{Z}$ be the ring of integers modulo n. Calculate $\mathrm{Aut}(R)$.

2.2.4 Show that for each of the rings $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ the automorphism group is trivial, but the automorphism group of $\mathbb{C}$ is not. [*Hint:* If $\alpha, \beta \in \mathbb{R}$,

then $\alpha \le \beta \iff \alpha + \xi^2 = \beta$ for some $\xi \in \mathbb{R}$; use this to show that each automorphism of $\mathbb{R}$ preserves the ordering of $\mathbb{R}$. In the case of $\mathbb{C}$ it can be shown that $\mathrm{Aut}(\mathbb{C})$ is uncountably infinite, but this is quite difficult.]

2.2.5 If G is a finite p-group which acts on another finite p-group $H \neq 1$ preserving the group structure, show that $\mathrm{fix}(G) \neq 1$. In particular, if G is a finite p-group acts on a finite-dimensional vector space V over a finite field of characteristic p, then there exists $v \neq 0$ in V which is fixed by every $x \in G$.

EXAMPLE 2.2.3. (Automorphisms of ordered sets) If Ω is a set with a partial (or total) ordering $\le$, then the *order-automorphisms* of $(\Omega, \le)$ are the permutations x of Ω which preserve the ordering in the sense:

$$\alpha^x \le \beta^x \iff \alpha \le \beta$$

for all $\alpha, \beta \in \Omega$. We shall denote the group of all order-automorphisms of $(\Omega, \le)$ by $\mathrm{Aut}(\Omega, \le)$.

Exercises

2.2.6 If $(\Omega, \le)$ is a finite totally ordered set, show that $\mathrm{Aut}(\Omega, \le)$ is trivial.

2.2.7 Show that $\mathrm{Aut}(\mathbb{Z}, \le)$ (with the usual ordering) is an infinite cyclic group. What is $\mathrm{Aut}(\mathbb{Z}, \mid\ )$ in the case that $\mid$ is the partial ordering defined by: $m \mid n \iff m$ divides n?

2.2.8 Show that $G := \mathrm{Aut}(\mathbb{Q}, \le)$ (with the usual ordering) is a highly homogeneous subgroup of $Sym(\mathbb{Q})$, but G is not 2-transitive. Prove that $G_\alpha \cong G \times G$ for each $\alpha \in \Omega$. (See also Exercise 7.1.2.)

2.2.9 (For those who know some topology) Let T be a topological space. We define a permutation f of the underlying set of T to be an automorphism of T if it preserves the topology of T in the sense that whenever U is a subset of T:

$$U^f \text{ is open} \iff U \text{ is open.}$$

Show that f is an automorphism $\iff$ f is a homeomorphism (that is, a bijection of T onto itself such that both f and f^{-1} are continuous).

2.3 Graphs

Graphs come in two principal types: directed graphs and nondirected graphs. We shall refer to directed graphs as *digraphs* and use the term *graph* to refer to nondirected graphs. The following is a list of formal definitions.

A *digraph* $\mathcal{G}$ is a pair (V, E) of sets V (of *vertices* or "nodes") and E (of *edges*) where $E \subseteq V \times V$; the digraph $\mathcal{G}$ is said to be *finite* if V is finite,

and otherwise is *infinite*. An edge $(\alpha, \beta) \in E$ is said to *join* α to β, and β is *adjacent* to α; note that edges of the form (α, α) are permitted. The *out-degree* of α is the number of vertices β which are adjacent to α, and the *in-degree* of α is the number of vertices β to which α is adjacent. If α and β are vertices of a digraph $\mathcal{G}$, then a *directed path* in $\mathcal{G}$ from α to β of *length* d is a list of $d + 1$ vertices

$$\alpha_0 = \alpha, \alpha_1, \ldots, \alpha_d = \beta$$

such that $(\alpha_{i-1}, \alpha_i) \in E$ for $i = 1, \ldots, d$. If we only assume that either (α_{i-1}, α_i) or (α_i, α_{i-1}) lies in E, then the path is called *undirected*. The path is called *simple* if the vertices $\alpha_0, \alpha_1, \ldots, \alpha_d$ are distinct with the possible exception that α_0 may equal α_d. A *circuit* in $\mathcal{G}$ is a path of length $d \geq 1$ in which the first and last vertices are equal: $\alpha_0 = \alpha_d$.

A *graph* is a digraph with no edges of the form (α, α) and with the property that $(\alpha, \beta) \in E$ implies $(\beta, \alpha) \in E$. In a graph the in-degree and out-degree of a given vertex are equal and are referred to as the *degree*. A graph is *connected* if for all $\alpha, \beta \in V$ there is a path from α to β. (In a graph we clearly do not have to distinguish between directed and nondirected paths, but for digraphs there are two corresponding notions: strongly connected and weakly connected. See Sect. 3.2). A *tree* is a connected graph with no simple circuits of length greater than 2 (no graph has a circuit of length 1, but every edge (α, β) gives rise to a circuit α, β, α of length 2).

It is often convenient to use simple diagrams to represent graphs: vertices are represented as points, and edges are represented by lines joining the points. In the case of a digraph which is not a graph, an edge (α, β) is represented by a line with an arrow from the point representing α to the point representing β.

Exercises

2.3.1 If $\mathcal{G}$ is a connected graph with uncountably many vertices, show that at least one vertex has infinite degree.

2.3.2 If $\mathcal{G} = (V, E)$ is a finite connected graph, show that $|V| \leq |E| + 1$, and that equality holds exactly when $\mathcal{G}$ is a tree.

Now suppose that G is a group acting on the vertex set V of a digraph $\mathcal{G} = (V, E)$. Then we can define an action of G on $V \times V$ by $(\alpha, \beta)^x := (\alpha^x, \beta^x)$ for all $(\alpha, \beta) \in V \times V$ and $x \in G$. We shall say that G preserves the adjacency structure of $\mathcal{G}$ if $E^x = E$ for all $x \in G$ (and so G also acts on E if $E \neq \emptyset$). The set of all permutations of V which preserve the adjacency structure of $\mathcal{G}$ forms a group called the *automorphism* group of $\mathcal{G}$; it is denoted by $\mathrm{Aut}(\mathcal{G})$.

Exercises

2.3.3 Show that the automorphism group of the graph in Fig. 2.1(a) has order 20. Is its action on the vertex set primitive? [*Hint:* First show

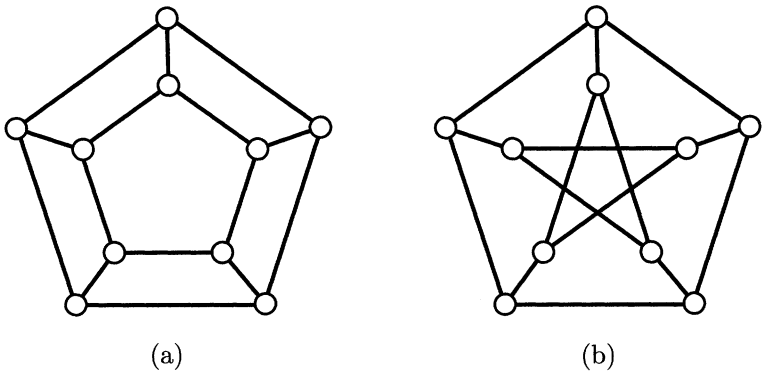


FIGURE 2.1.

that the automorphism group is transitive on the vertex set and then examine the stabilizer of a point.]

2.3.4 The graph in Fig. 2.1(b), known as the Petersen graph, has many interesting properties. Show that its automorphism group A has order 120 and that A acts primitively on the set of vertices. Show that the stabilizer of a vertex has 3 orbits, of lengths 1, 3 and 6, respectively. Is the action of A on the set of edges primitive?

2.3.5 Consider the automorphism group of the graph in Fig. 2.2. What can you say about the actions of this group on the set of 14 vertices and on the set of 21 edges?

2.3.6 Consider the digraph with vertex set $\mathbb{Z}$ and edge set $\{(i, i+1) \mid i \in \mathbb{Z}\}$. Is the automorphism group primitive?

2.3.7 Let $n \geq 3$. Consider the graph $\mathcal{G}$ whose vertex set V is the set of all 2-cycles $(\alpha\beta)$ in S_n, and where two distinct vertices are adjacent exactly when they commute. Show that $\mathrm{Aut}(\mathcal{G})$ is a primitive but

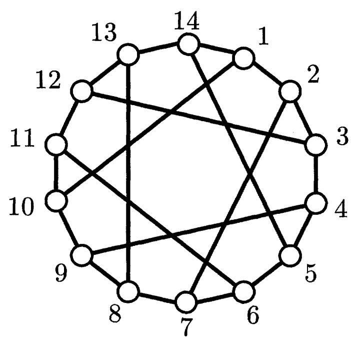


FIGURE 2.2.

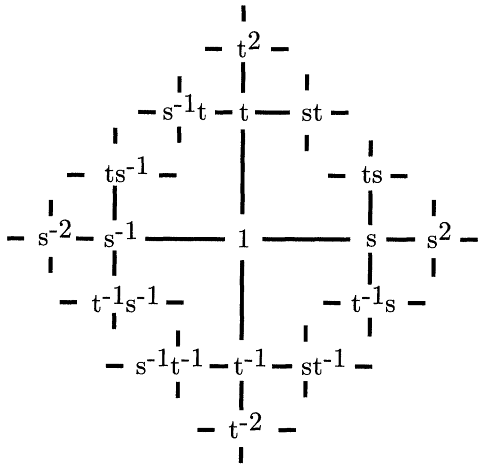


FIGURE 2.3. The Cayley graph for the free group on generators s, t.

not 2-transitive group on V if $n \neq 4$, and that $\mathrm{Aut}(\mathcal{G}) \cong S_n$ if $n > 2$. [*Hint:* Compare with Example 2.1.2.]

2.3.8 Is the graph constructed in the previous exercise for $n = 5$ isomorphic to the Petersen graph [Fig. 2.1(b)]?

2.3.9 If $\mathcal{T}$ is a finite tree, show that either $\mathrm{Aut}(\mathcal{T})$ fixes some vertex α, or there is an edge (β, γ) such that each $x \in \mathrm{Aut}(\mathcal{T})$ fixes (β, γ) or maps (β, γ) onto its reverse (γ, β).

2.3.10 Let G be a group and R be a subset of G. Consider the graph with vertex set G whose edge set consists of all pairs (a, ra) $(a \in G, r \in R \cup R^{-1})$; we call this the *Cayley graph* and denote it by $\mathrm{Cayley}(G, R)$. Fig. 2.3 displays a fragment of a particular Cayley graph. Prove that $\mathrm{Cayley}(G, R)$ is connected $\iff$ R generates G. Show that $\mathrm{Aut}(\mathrm{Cayley}(G, R))$ contains the right regular representation of G in $Sym(G)$. Sketch $\mathrm{Cayley}(G, R)$ where $G = S_3$ and $R = \{(12), (123)\}$.

2.3.11 Let R be a subset of a group G and suppose that $R \cap R^{-1} = \emptyset$. Show that $\mathrm{Cayley}(G, R)$ is a tree $\iff$ G is a free group and R is a set of free generators for G.

2.4 Relations

You will be familiar with a variety of relations, such as: congruence modulo m on the set $\mathbb{Z}$; linear dependence between k vectors in $\mathbb{R}^n$; a partial ordering such as containment ($\subseteq$) on the set of subsets of a fixed set; and numerous others. We can describe all such relations set-theoretically in a

rather bland way as follows. For each integer $r \geq 1$, an *r-ary relation* on a set Ω is a subset $\Lambda \subseteq \Omega^r$ where $\Omega^r = \Omega \times .. \times \Omega$ (r times). Strictly speaking, the relations just defined are *finitary* relations. It is also possible to define infinitary relations in an analogous way, but in what follows "relation" will always refer to the finitary relations defined above. It is common to use the terms unary, binary and ternary to refer to the cases 1-ary, 2-ary and 3-ary, respectively.

EXAMPLE 2.4.1. The usual ordering on $\mathbb{R}$ is a binary relation given by $\Lambda := \{(\alpha, \beta) \in \mathbb{R}^2 \mid \alpha \leq \beta\}$.

EXAMPLE 2.4.2. The relation "linearly dependent for k vectors" on a vector space V is a k-ary relation given by a set which consists simply of k-tuples of linearly dependent vectors.

EXAMPLE 2.4.3. If $\phi : \Gamma \to \Omega$ is a function "in k variables" from a subset $\Gamma \subseteq \Omega^k$ into Ω, then there is a canonical $(k+1)$-ary relation (the "graph" of ϕ) associated with ϕ, namely,

$$\{(\alpha_1, \ldots, \alpha_k, \phi(\alpha_1, \ldots, \alpha_k)) \mid (\alpha_1, \ldots, \alpha_k) \in \Gamma\}.$$

Clearly this relation completely defines ϕ (including its domain Γ). Do not confuse this meaning of "graph" with the graphs considered in the previous section.

EXAMPLE 2.4.4. A special case of the last relation is where ϕ is the binary operation on a group G; the associated ternary relation on G is

$$\{(x, y, xy) \mid x, y \in G\}.$$

We also have the binary relation

$$\{(x, x^{-1}) \mid x \in G\}$$

corresponding to inversion, and the unary relation $\{1\}$ which specifies the identity of the group.

Exercise

2.4.1 Specify all the operations in a vector space V over a field F in terms of relations on V. [*Hint:* To express scalar multiplication you will need one relation for each scalar.]

We can use relations to define permutation groups. Let $\mathcal{R}$ be a set of relations on a nonempty set Ω. Now $Sym(\Omega)$ acts (componentwise) on Ω^k for each k, so we can consider the set G of all permutations of Ω which map each of the relations in $\mathcal{R}$ onto itself. It is easily seen that G is a subgroup of $Sym(\Omega)$; G is called the group of *$\mathcal{R}$-preserving permutations* of Ω, or the *automorphism group of the relational structure* $(\Omega; \mathcal{R})$, and is

denoted by $\mathrm{Aut}(\Omega; \mathcal{R})$. For instance, in Example 2.2.3 and Exercises 2.2.7 and 2.2.8 we looked at the automorphism groups of various order relations. The automorphism group of a graph is just the automorphism group of a relational structure on the set of vertices where we have a single binary relation ρ with $(\alpha, \beta) \in \rho \iff \{\alpha, \beta\}$ is an edge. Similarly a group G preserves various operations on Ω if it preserves the associated relations; for an algebraic structure such as a group, the permutations of the underlying set which preserve the relations are the usual automorphisms discussed in Sect. 2.2. There is a more detailed discussion of relational structures in Sect. 9.5 and 9.6.

EXAMPLE 2.4.5. Let H be a group, and let Γ be the ternary relation on H associated with the group operation (see Example 2.4.4). If G is the group of permutations of H which preserve Γ, then

$$x \in G \iff x \in Sym(H) \text{ and } \Gamma^x = \Gamma.$$

However $\Gamma^x = \Gamma$ implies that $(u^x, v^x, (uv)^x) \in \Gamma$ for all $u, v \in H$, and so $u^x v^x = (uv)^x$ for all $u, v \in H$. Hence each $x \in G$ is an automorphism of the group H. The converse is easy to verify, and so G consists of exactly the group automorphisms of H.

Exercise

2.4.2 The *Fano plane* $\mathcal{F}$ is represented in Fig. 2.4. The plane consists of seven "points" (labelled 1 to 7 in the figure) and seven "lines" each of which is a triple of points (in the diagram these correspond to the triples which lie on straight lines and the triple $\{2, 4, 6\}$ on the circle). Three points are *collinear* if they lie on the same line. The automorphism group $\mathrm{Aut}(\mathcal{F})$ of the Fano plane consists of all permutations of the points which preserve the relation of collinearity. Find a set of generators for $\mathrm{Aut}(\mathcal{F})$ and show that $|\mathrm{Aut}(\mathcal{F})| = 168$. Is the action

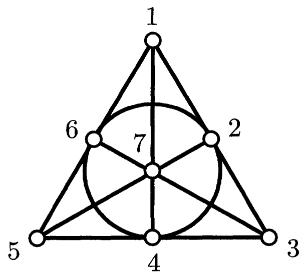


FIGURE 2.4. The Fano plane

of $\mathrm{Aut}(\mathcal{F})$ on the set of points equivalent to its action on the set of lines?

Conversely, if a group G acts on a set Ω, each of its orbits on Ω^k defines a relation preserved by G. Thus every permutation group is contained in the automorphism group of a relational structure; in general it is not the full automorphism group of this structure. A subgroup G of $Sym(\Omega)$ is called *closed* if it is the automorphism group of some set of relations on Ω; and it is called *k-closed* ($k = 1, 2, \ldots$) if it is the automorphism group of some set of k-ary relations. In many situations these groups possess useful properties which are not shared by all permutation groups.

Exercises

2.4.3 If Ω is finite, show that every subgroup of $Sym(\Omega)$ is closed.

2.4.4 Describe all 1-closed permutation groups.

2.4.5 Let G be a subgroup of $Sym(\Omega)$ and let G_0 denote the intersection of all 2-closed subgroups of $Sym(\Omega)$ which contain G (we call the subgroup G_0 the *2-closure* of G). Show that G_0 is a subgroup of $Sym(\Omega)$ and that:
 (i) if G is finite then so is G_0;
 (ii) if each element in G has finite odd order, then so does each element of G_0;
 (iii) if G is abelian, then so is G_0;
 (iv) if G is a p-group, then so is G_0.

2.4.6 If G is a closed subgroup of $Sym(\Omega)$ and $H \leq G$, show that the centralizer $C_G(H)$ is closed, but that, in general, the normalizer $N_G(H)$ is not closed. Is $N_G(H)$ closed when H is closed?

The idea of closure defined above can be related to a topological construction as follows. Consider the symmetric group $S := Sym(\mathbb{N})$. Let $S(i)$ denote the pointwise stabilizer of the set $\{0, 1, \ldots, i-1\}$ for $i = 0, 1, \ldots$. We define the distance $d(x, y)$ between two distinct permutations x, y in S to be 2^{-k} where k is the greatest integer such that xy^{-1} and yx^{-1} both lie in $S(k)$ and we put $d(x, x) = 0$.

Exercises

2.4.7 Show that for all $x, y, z \in S$:
 (i) $d(x, y) = 0 \iff x = y$;
 (ii) $d(x, y) = d(y, x)$;
 (iii) $d(x, y) \leq \max\{d(x, z), d(y, z)\}$.

Thus (S, d) is a metric space; indeed, (iii) is a strong form of the triangle inequality and shows that we have an *ultrametric*. Show that the functions $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous, with respect to this metric, on $S \times S$ and S, respectively.

2.4.8 Show that any Cauchy convergent sequence in (S, d) converges, and so (S, d) is a complete metric space.

2.4.9 Show that a subgroup G of $Sym(\mathbb{N})$ is closed in the sense described earlier in this section if and only if it is closed as a subset of the metric space (S, d).

2.4.10 (For those who know some topology.) Let $S := Sym(\Omega)$ for an arbitrary set Ω, and consider the topology on S obtained by taking as a basis of open sets all sets of the form $xS_{(\Delta)} \cap S_{(\Delta)}x$ ($x \in S$ and Δ a finite subset of Ω). When $\Omega = \mathbb{N}$, show that this is the same topology as that induced by the metric in Exercise 2.4.7, and prove that the analogues of Exercises 2.4.7 and 2.4.9 hold in the general case. (If Ω is uncountably infinite, then it can be shown that the topology on this space is not induced by any metric.)

2.5 Semidirect Products

The wreath product constructions which we shall consider in the next two sections are of fundamental importance in the study of permutation groups. However, to understand those constructions we must first look at the simpler construction of semidirect products.

The notion of a semidirect product of two groups generalizes the idea of a direct product. Let H and K be groups and suppose that we have an action of H on K which respects the group structure on K; so for each $x \in H$ the mapping $u \mapsto u^x$ is an automorphism of K. Put

$$G := \{(u, x) \mid u \in K, x \in H\}$$

and define a product on G by

$$(u, x)(v, y) := (uv^{x^{-1}}, xy)$$

for all $(u, x), (v, y) \in G$.

Exercise

2.5.1 Check that this product is associative, and hence show that G is a group under this operation with identity element (1,1) and with $(u, x)^{-1} = ((u^x)^{-1}, x^{-1})$.

It is readily seen that G contains subgroups $H^* := \{(1, x) \mid x \in H\}$ and $K^* := \{(u, 1) \mid u \in K\}$ which are isomorphic to H and K, respectively, and that $G = K^*H^*$ and $K^* \cap H^* = 1$. Moreover, K^* is normal in G and the way that H^* acts on K^* by conjugation reflects the original action of H on K, namely,

$$(1, x)^{-1}(u, 1)(1, x) = (u^x, 1)$$

for all $x \in H$ and $u \in K$.

We call G the *semidirect product of* K *by* H and shall use the notation $K \rtimes H$ to denote G. Of course the semidirect product depends implicitly

on the action of H on K even though the action is not specified in the notation. Clearly $|G| = |H|\,|K|$.

Exercises

2.5.2 Show that the direct product $K \times H$ is a particular case of the semidirect product.

2.5.3 Suppose that G is a group and K and H are subgroups with $K \lhd G$, $G = KH$ and $K \cap H = 1$. Show that G is isomorphic to $K \rtimes H$ where the implied action of H on K is the conjugation action in G. (G is called a *split extension* of K by H, so every split extension is isomorphic to a corresponding semidirect product.)

2.5.4 Let G be a split extension of a subgroup H and normal subgroup K. Consider the action of G (by right multiplication) on the set of right cosets of H. Show that the image of K in this representation is a regular permutation group.

2.5.5 Suppose that $G \leq Sym(\Omega)$ and let $\alpha \in \Omega$. If G has a regular normal subgroup K, show that G is a split extension of K and G_α. (The natural action of G_α on Ω is equivalent to the conjugation action of G_α on K by Exercise 1.6.16.)

2.5.6 Let K be a regular subgroup of $Sym(\Omega)$, and let C and N, respectively, denote the centralizer and normalizer of K in $Sym(\Omega)$ (N is called the *holomorph* of K). Show that C is a regular subgroup isomorphic to K and that $N/C \cong \mathrm{Aut}(K)$. (In principle, one way in which we could compute the automorphism group is to construct the regular representation of the group in question and then apply this result. In practice, this does not seem to be very useful.)

2.5.7 Calculate the holomorphs for the cyclic group of order 4, for the noncyclic group of order 4 and for S_3.

2.5.8 Let $G \leq Sym(\Omega)$ have a regular normal subgroup R and let $\alpha \in \Omega$. Show that G is primitive $\iff$ no proper nontrivial subgroup of R is normalized by G_α.

2.5.9 Let K be a nonabelian group and put $G = K \times K$. Consider the action of G on K given by $u^{(x,y)} := x^{-1}uy$ $(u \in K, (x,y) \in G)$. Show that the normal subgroups $K \times 1$ and $1 \times K$ both act regularly, and that the action of G is primitive exactly when K is simple.

2.6 Wreath Products and Imprimitive Groups

The notion of a wreath product arises very naturally in the study of imprimitive groups. For example, let Σ be a partition of a set Ω into equal-sized subsets. Then the group G of automorphisms of Σ consists of all $x \in Sym(\Omega)$ with the property that if $\Delta \subseteq \Omega$ then

$$\Delta \in \Sigma \iff \Delta^x \in \Sigma.$$

Clearly, G also acts on Σ. If we define B to be the kernel of this latter action, then it is easy to see that B is isomorphic to the direct product of $|\Sigma|$ copies of $Sym(\Delta)$ where $\Delta \in \Sigma$, and that $G \cong B \rtimes Sym(\Sigma)$ where $Sym(\Sigma)$ acts on B by permuting the components of the elements of B in a natural way. This gives a fairly simple description of G. More generally, if H is an imprimitive group which has Σ as a system of blocks, then $H \leq G$, and so H will also decompose, although the details of the decomposition are generally much more complicated for H than those for G. The wreath product construction which we now consider is a refinement of the construction we have just made for G.

If Γ and Δ are nonempty sets then we write $\mathrm{Fun}(\Gamma, \Delta)$ to denote the set of all functions from Γ into Δ. In the case that K is a group, we can turn $\mathrm{Fun}(\Gamma, K)$ into a group by defining a product "pointwise":

$$(fg)(\gamma) := f(\gamma)g(\gamma) \quad \text{for all } f, g \in \mathrm{Fun}(\Gamma, K) \text{ and } \gamma \in \Gamma$$

where the product on the right is in K. In the case that Γ is finite of size m, say $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$, then the group $\mathrm{Fun}(\Gamma, K)$ is isomorphic to K^m (a direct product of m copies of K) via the isomorphism $f \mapsto (f(\gamma_1), \ldots, f(\gamma_m))$.

Let K and H be groups and suppose H acts on the nonempty set Γ. Then the *wreath product* of K by H with respect to this action is defined to be the semidirect product $\mathrm{Fun}(\Gamma, K) \rtimes H$ where H acts on the group $\mathrm{Fun}(\Gamma, K)$ via

$$f^x(\gamma) := f(\gamma^{x^{-1}}) \quad \text{for all } f \in \mathrm{Fun}(\Gamma, K), \gamma \in \Gamma \text{ and } x \in H.$$

We denote this group by $K \; wr_\Gamma \; H$, and call the subgroup

$$B := \{(f, 1) \mid f \in \mathrm{Fun}(\Gamma, K)\} \cong \mathrm{Fun}(\Gamma, K)$$

the *base group* of the wreath product.

Again, it is helpful to look at the case where Γ is finite, say $\Gamma = \{1, 2, \ldots, m\}$. In this case we can identify the base group B with the direct product $K \times \ldots \times K$ (m factors), and the action of H on B corresponds to permuting the components:

$$(u_1, \ldots, u_m)^x = (u_{1'}, \ldots u_{m'}) \quad \text{when } x = \begin{pmatrix} 1 & \ldots & m \\ 1' & \ldots & m' \end{pmatrix}$$

for all $(u_1, \ldots, u_m) \in B$ and $x \in H$. Clearly, $|K \; wr_\Gamma \; H| = |K|^m \, |H|$.

Exercises

2.6.1 Verify that the definition of f^x does give an action of H on $\mathrm{Fun}(\Gamma, K)$ which respects the group structure. (Why has it been necessary to introduce x^{-1} into the definition rather than x?)

2.6.2 Let $G \leq Sym(\Omega)$ be an imprimitive group and let $\Sigma = \{\Gamma_i \mid i \in I\}$ be a system of blocks for G. Let H denote the kernel of the action of G on Σ, and let K be the subgroup of $Sym(\Omega)$ consisting of all

$x \in Sym(\Omega)$ such that $\Gamma_i^x \in \Sigma$ for each $i \in I$. Show that $K \cong Sym(\Gamma)\ wr_I\ Sym(I)$ where $|\Gamma| = |\Gamma_i|$ for each $i \in I$, and so G can be embedded in $Sym(\Gamma)\ wr_I\ Sym(I)$ in such a way that H consists of the set of elements of G which are mapped into the base group.

2.6.3 If $G \leq Sym(\Omega)$ is an imprimitive subgroup which is maximal in the sense that it is not contained in any larger imprimitive group, show that G is isomorphic to a wreath product of the form $Sym(\Gamma)\ wr_I\ Sym(I)$ where G has a system of blocks indexed by I and each block has size $|\Gamma|$.

2.6.4 Show that the group G considered in the preceding exercise is actually a maximal subgroup of $Sym(\Omega)$ in the case Ω is finite and $|I|$ and $|\Gamma|$ are at least 2. Is this also true when Ω is infinite?

In the special case of a wreath product where the group H acts regularly on itself, we write $K\ wr\ H$ in place of $K\ wr_H\ H$; this is called the *standard wreath product*. This particular wreath product has a useful property described in the following theorem.

Theorem 2.6A (Universal embedding theorem). *Let G be an arbitrary group with a normal subgroup N, and put $K := G/N$. Then there is an embedding $\phi : G \to N\ wr\ K$ such that ϕ maps N onto* $\mathrm{Im}\ \phi \cap B$ *where B is the base group of $N\ wr\ K$. (Thus $N\ wr\ K$ contains an isomorphic copy of every extension G of N by K.)*

PROOF. Let $\psi : G \to K$ be a homomorphism of G onto K with kernel N. Let $T := \{t_u \mid u \in K\}$ be a set of right coset representatives of N in G such that $\psi(t_u) = u$ for each $u \in K$. If $x \in G$, then $\psi(t_u x) = \psi(t_u)\psi(x) = u\psi(x)$ and so $t_u x t_{u\psi(x)}^{-1} \in N$. Thus for each $x \in G$ we can define a function $f_x : K \to N$ by

$$f_x(u) := t_u x t_{u\psi(x)}^{-1} \quad \text{for all } u \in K$$

and put

$$\phi(x) := (f_x, \psi(x)) \in N\ wr\ K.$$

We claim that this defines an embedding ϕ of G into $N\ wr\ K$ with the required properties.

First, ϕ is a homomorphism. Indeed, if $x, y \in G$, then

$$\phi(x)\phi(y) = (f_x f_y^{\psi(x)^{-1}}, \psi(xy))$$

because ψ is a homomorphism. On the other hand, for all $u \in K$, we have

$$\begin{aligned} f_{xy}(u)t_{u\psi(xy)} &= t_u xy = \{f_x(u)t_{u\psi(x)}\}y \\ &= f_x(u)f_y(u\psi(x))t_{u\psi(x)\psi(y)} \\ &= f_x(u)f_y^{\psi(x)^{-1}}(u)t_{u\psi(xy)} \end{aligned}$$

and so $f_{xy} = f_x f_y^{\psi(x)^{-1}}$. Hence

$$\phi(x)\phi(y) = (f_{xy}, \psi(xy)) = \phi(xy)$$

as required. Second, $\ker \phi = 1$ because $\phi(x) = 1$ implies that $f_x = 1$ and $\psi(x) = 1$, and so $x = t_1^{-1} f_x(1) t_{1\psi(x)} = 1$. Finally, $\phi(x)$ lies in B when $\psi(x) = 1$, and this happens exactly when $x \in N$. □

Exercise

2.6.5 Suppose that G is any extension of a normal subgroup N by a group $K \neq 1$, and that N can be embedded as a transitive subgroup in $Sym(\Delta)$. Show that G can be embedded as an imprimitive subgroup in $Sym(\Omega)$ where $\Omega = \Delta \times K$.

Exercises 2.6.2 and 2.6.5 show how wreath products arise in the study of imprimitive groups. They can also be used to construct groups with specific properties as we now show.

Consider the wreath product $G := K \; wr_\Gamma \; H$. If K acts on a set Δ, then we can define an action of G on $\Delta \times \Gamma$ by

$$(\delta, \gamma)^{(f,u)} := (\delta^{f(\gamma)}, \gamma^u) \quad \text{for all } (\delta, \gamma) \in \Delta \times \Gamma$$

where $(f, u) \in \mathrm{Fun}(\Gamma, K) \rtimes H = K \; wr_\Gamma \; H$.

Exercises

2.6.6 Verify that this is an action of G on $\Delta \times \Gamma$, and that it is faithful $\iff$ the action of K on Δ is faithful.

2.6.7 Prove the associativity property: if we also have a group L acting on Λ, then

$$(K \; wr_\Gamma \; H) \; wr_\Lambda \; L \cong K \; wr_{\Gamma \times \Lambda} \; (H \; wr_\Lambda \; L)$$

with the appropriate action of $H \; wr_\Lambda \; L$ on $\Gamma \times \Lambda$.

EXAMPLE 2.6.1. (The Sylow p-subgroups of a finite symmetric group) Fix a prime p, and let C be a cyclic group of order p acting regularly on a set Δ of size p. Define recursively: $P_1 = C$ acting on Δ; and $P_m = P_{m-1} \; wr_\Delta \; C$ acting on Δ^m for $m \geq 2$. Thus P_m has order $p^{\mu(m)}$ where $\mu(1) = 1$ and $\mu(m) = p\mu(m-1) + 1$; so simple induction shows that $\mu(m) = (p^m - 1)/(p-1)$. Since P_m acts faithfully on Δ^m this shows that $Sym(p^m) (\cong Sym(\Delta^m))$ contains a subgroup isomorphic to this iterated wreath product P_m.

On the other hand, suppose that n is a positive integer, and write n to the base p:

$$n = n_0 + n_1 p + \ldots + n_k p^k \quad \text{where } 0 \leq n_i < p \text{ for each } i.$$

Then it follows from Exercise 2.6.8 below that the Sylow p-subgroups of S_n have order $p^{\nu(n)}$ where

$$\nu(n) = n_1 + n_2(p^2 - 1)/(p - 1) + \ldots + n_k(p^k - 1)/(p - 1).$$

Thus we can construct a Sylow p-subgroup for S_n as follows. Partition the set $\{1, 2, \ldots, n\}$ into n_0 subsets of size 1, n_1 subsets of size p, ..., n_k subsets of size p^k. For each of the subsets of size p^m $(m = 1, \ldots, k)$ apply the iterated wreath product construction above to obtain a subgroup of order $p^{\mu(m)}$ in S_n whose support is this subset of size p^m. Then the direct product of all the subgroups obtained in this way is a group of order p^h where

$$h = \sum n_m \mu(m) = \sum n_m(p^m - 1)/(p - 1) = \nu(n)$$

and so we have a Sylow p-subgroup of S_n.

We illustrate this construction in the case where $n = 15$ and $p = 3$. Since $n = 2 \cdot 3 + 1 \cdot 3^2$ we partition the points into the subsets $\{1, 2, 3\}$, $\{4, 5, 6\}$ and $\{7, 8, \ldots, 15\}$. For the first two of these subsets we can construct subgroups of order 3, for example, $\langle(1\ 2\ 3)\rangle$ and $\langle(4\ 5\ 6)\rangle$. For the last set we construct a wreath product of a group of order 3 by a group of order 3, for example, the split extension

$$\langle(7\ 8\ 9), (10\ 11\ 12), (13\ 14\ 15)\rangle\langle(7\ 10\ 13)(8\ 11\ 14)(9\ 12\ 15)\rangle$$

which has order 3^4. Since these three subgroups have mutually disjoint supports, the subgroup which they generate is their direct product. It is a Sylow 3-subgroup (of order 3^6) for S_{15}.

Exercises

2.6.8 Let n be a positive integer and p a prime. Suppose that

$$n = n_0 + n_1 p + \ldots + n_k p^k \quad \text{where } 0 \le n_i < p \text{ for each } i.$$

Show that the largest power of p which divides $n!$ is $p^{\nu(n)}$ where

$$\nu(n) = \sum_{i=0}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor = n_1 + n_2 \frac{(p^2 - 1)}{(p - 1)} + \ldots + n_k \frac{(p^k - 1)}{(p - 1)} < \frac{n}{p - 1}.$$

2.6.9 Construct a Sylow 2-subgroup for S_{14}.

2.6.10 Show that the iterated wreath product P_m defined above can be generated by m elements.

2.7 Primitive Wreath Products

The construction in the previous section showed how wreath products arise as imprimitive groups. Wreath products also play an important role in the

study of primitive permutation groups. They will be central to our work in Chap. 4.

We first outline the general idea. Let H and K be groups acting on sets Γ and Δ, respectively. Then $\mathrm{Fun}(\Gamma, K)$ is isomorphic to the direct product of $|\Gamma|$ copies of K and as such acts in a natural way on the Cartesian product Ω of $|\Gamma|$ copies of Δ. We also have H acting on Ω in a natural way (by permuting the components). These two actions can be combined to give an action of $K \; wr_\Gamma \; H = \mathrm{Fun}(\Gamma, K) \rtimes H$ on Ω, but we have to be careful to make the two actions compatible. As we shall see, the action is primitive under certain mild conditions. The details of the construction are as follows.

Put $\Omega := \mathrm{Fun}(\Gamma, \Delta)$ and $W := K \; wr_\Gamma \; H = \mathrm{Fun}(\Gamma, K) \rtimes H$; we want to define an action of W on Ω. For each $\phi \in \Omega$ and each $(f, x) \in W$ we define $\phi^{(f,x)}$ by putting

$$\phi^{(f,x)}(\gamma) := \phi(\gamma^{x^{-1}})^{f(\gamma^{x^{-1}})} \quad \text{for each } \gamma \in \Gamma.$$

Clearly $\phi^{(1,1)} = \phi$, and $(f, x)(g, y) = (fg^{x^{-1}}, xy)$ in W. Thus to prove that we have an action it remains to show that $\phi^{(f,x)(g,y)} = \phi^{(fg^{x^{-1}},xy)}$ for all $\phi \in \Omega$ and all $(f, x), (g, y) \in W$. However, on one hand, we have

$$\phi^{(f,x)(g,y)}(\gamma^{xy}) = \phi^{(f,x)}(\gamma^x)^{g(\gamma^x)} = \phi(\gamma)^{f(\gamma)g(\gamma^x)}$$

while on the other

$$\phi^{(fg^{x^{-1}},xy)}(\gamma^{xy}) = \phi(\gamma)^{f(\gamma)g^{x^{-1}}(\gamma)} = \phi(\gamma)^{f(\gamma)g(\gamma^x)}$$

and so replacing γ by $\gamma^{(xy)^{-1}}$ gives the required identity. This action of $K \; wr_\Gamma \; H$ on Ω is called the *product action* of the wreath product.

It is easily verified that the product action of $W := K \; wr_\Gamma \; H$ is faithful exactly when the given actions of H and K are both faithful. The degree $|\Omega|$ of W equals $|\Delta|^{|\Gamma|}$; this is clear if Δ and Γ are finite, and it can also be proved in the infinite cases. The next lemma gives a simple criterion for this action to be primitive. Recall that a group K is both primitive and regular only when K is a cyclic group of prime order.

Lemma 2.7A. *Suppose that H and K are nontrivial groups acting on the sets Γ and Δ, respectively. Then the wreath product $W := K \; wr_\Gamma \; H$ is primitive in the product action on $\Omega := \mathrm{Fun}(\Gamma, \Delta)$ if and only if:*

(i) *K acts primitively but not regularly on Δ; and*

(ii) *Γ is finite and H acts transitively on Γ.*

PROOF. Let B be the base group of W and put

$$H_0 := \{(1, x) \in W \mid x \in H\}$$

so W is the split extension BH_0. Fix $\delta \in \Delta$, and define $\phi_\delta \in \Omega$ by $\phi_\delta(\gamma) := \delta$ for all γ. Then

$$L := \{(f, x) \in W \mid f(\gamma) \in K_\delta \quad \text{for all } \gamma\}$$

is the stabilizer in W of the point ϕ_δ. It follows from Corollary 1.5A that W is primitive if and only if W is transitive and L is a maximal subgroup of W.

We first prove the necessity of conditions (i) and (ii). First, if H is not transitive and Σ is an orbit of H in Γ, then

$$M := \{(f,1) \in B \mid f(\gamma) \in K_\delta \quad \text{for all } \gamma \in \Sigma\}$$

is a subgroup of B which is normalized by H, and $L < MH_0 < W$; thus W is not primitive. On the other hand, if Γ is infinite, and we define

$$B_0 := \{(f,1) \in B \mid f \text{ has finite support on } \Gamma\}$$

then $B_0 \triangleleft W$ and $L < LB_0 < W$, so W is not primitive. Similarly, if K is intransitive with an orbit Π then

$$\{(f,x) \in W \mid f(\gamma) \in K_\delta \quad \text{for all } \gamma \in \Pi\}$$

is a subgroup of W lying strictly between L and W, and so again W is not primitive. In the case where K is transitive but imprimitive there exists R such that $K_\delta < R < K$, and then the subgroup

$$\{(f,x) \in W \mid f(\gamma) \in R \quad \text{for all } \gamma\}$$

lies strictly between L and W. Finally, in the case where K is regular the subgroup

$$D := \{(f,1) \in B \mid f(\gamma) = f(\gamma') \quad \text{for all } \gamma, \gamma'\}$$

is normalized by H_0 and then $L < DH_0 < W$. Thus in all these cases W is not primitive. This proves the necessity of conditions (i) and (ii).

Conversely, suppose that (i) and (ii) hold; we want to show that W is primitive. Clearly B, and hence W, is transitive. Thus it is enough to show that $L < M \le W$ implies that $M = W$. Since $W = BH_0 = BL$ we have $M = (M \cap B)L$. Therefore $M \cap B > L \cap B$ and so, for some γ_0, there exists $(f,1) \in M \cap B$ with $f(\gamma_0) \notin K_\delta$. Since K is primitive and not regular, $K_\delta = N_K(K_\delta)$ (see Exercise 2.7.1) and so for some $u \in K_\delta$ we have $f(\gamma_0)^{-1}uf(\gamma_0) \notin K_\delta$. Define $g \in \mathrm{Fun}(\Gamma, H)$ by $g(\gamma_0) := u$ and $g(\gamma) := 1$ for all $\gamma \ne \gamma_0$. Then $h := [f,g] \in ML$ where $h(\gamma_0) = [f(\gamma_0), u] \in KK_\delta$ and $h(\gamma) = 1$ for all $\gamma \ne \gamma_0$. Since K is primitive, K_δ is maximal, and so $K = \langle K_\delta, h(\gamma_0)\rangle$; therefore M contains the subgroup

$$B(\gamma_0) := \{(f,1) \in B \mid f(\gamma) = 1 \quad \text{for all } \gamma \ne \gamma_0\}.$$

However, it is readily seen that $(1,x)B(\gamma_0)(1,x)^{-1} = B(\gamma_0)$. Since $H_0 \le M$ and H is transitive on Γ we conclude that $B(\gamma) \le L$ for all $\gamma \in \Gamma$. Since Γ is finite we conclude that

$$B = \prod_{\gamma \in \Gamma} B(\gamma) \le M$$

and so $M = BH_0 = W$ as required. This shows that conditions (i) and (ii) are also sufficient. □

Exercises

2.7.1 Show that a primitive group G is not regular if and only if a point stabilizer G_α equals its normalizer $N_G(G_\alpha)$.

2.7.2 Find (up to equivalence) all primitive representations of $S_3\ wr\ S_2$. Note that not all of them are of the form described in Lemma 2.7A.

2.7.3 Let $H \leq Sym(\Gamma)$ and $K \leq Sym(\Delta)$ where Δ is finite, and consider the product action of $G := H\ wr_\Delta\ K$ on $\Omega := \mathrm{Fun}(\Gamma, \Delta)$. Suppose that H has m orbits on Γ. Show that G has $\frac{1}{|K|}\sum_{x\in K} m^{\kappa(x)}$ orbits on Ω where $\kappa(x)$ denotes the number of cycles of x. (See also Exercise 1.7.9.)

2.8 Affine and Projective Groups

The affine and projective groups constitute two interrelated infinite families of permutation groups. The groups arise naturally from affine and projective geometries and can also be defined algebraically. Since the geometry does not enter strongly into the smallest members of each family we shall begin with an algebraic introduction to these 1-dimensional groups.

If the underlying set on which we are acting is a field, then sets of permutations of certain natural types form subgroups of the symmetric group. Historically, these examples of permutation groups arose quite early in the subject; the first examples were given by Évariste Galois in 1830.

Let F be a field. Then it is straightforward to verify that the set A of all permutations of F of the form

$$t_{\alpha\beta} : \xi \mapsto \alpha\xi + \beta \quad (\alpha, \beta \in F \text{ and } \alpha \neq 0)$$

constitutes a subgroup of $Sym(F)$ (check this!) which is called the 1-dimensional *affine group* over F and is denoted by $AGL_1(F)$. In the special case where F is a finite field of order q, say, we have $|AGL_1(F)| = q(q-1)$. In this case, the notation $AGL_1(q)$ is often used in place of $AGL_1(F)$; there is no real ambiguity since all finite fields of the same order are isomorphic (see for example Lang (1993) Chap. V, Sect. 5).

Exercises

2.8.1 Verify the claims made above for $AGL_1(F)$. Show that the set of *translations* $t_{1\beta}$ ($\beta \in F$) forms a transitive normal abelian subgroup T of $AGL_1(F)$, and that $AGL_1(F)$ is a split extension of T by an abelian subgroup. Show that $AGL_1(F)$ itself is 2-transitive.

2.8.2 We may generalize the construction of $AGL_1(F)$ by replacing the field F by a general (possibly noncommutative) ring R with unity.

We define $AGL_1(R)$ to consist of all permutations of $Sym(R)$ of the form $\xi \mapsto \alpha\xi + \beta$ with $\alpha, \beta \in R$ where α is a unit in R. What results from the previous exercise remain valid for $AGL_1(R)$?

We now adjoin a new element (which we shall denote by ∞) to F to obtain a set $\Omega := F \cup \{\infty\}$, and identify $Sym(F)$ with the stabilizer of ∞ in $Sym(\Omega)$. Then we can define a *transitive extension* G of $AGL_1(F)$ in $Sym(\Omega)$ in the sense that G is transitive on Ω and $G_\infty = AGL_1(F)$. The group G consists of all *fractional linear mappings* of the form

$$t_{\alpha\beta\gamma\delta} : \xi \mapsto \frac{\alpha\xi + \beta}{\gamma\xi + \delta} \quad \text{with } \alpha, \beta, \gamma, \delta \in F \text{ and } \alpha\delta - \beta\gamma \neq 0$$

with the convention that $t_{\alpha\beta\gamma\delta}(\infty) = \alpha\gamma^{-1}$ and $t_{\alpha\beta\gamma\delta}(-\delta\gamma^{-1}) = \infty$.

Exercises

2.8.3 Show that with these rules for dealing with ∞ the fractional linear mappings are well-defined permutations of Ω.

2.8.4 Show that G is indeed a transitive subgroup of $Sym(\Omega)$ with $G_\infty = AGL_1(F)$, and $G_{\infty 0} = T$ (the group of translations). Conclude that G is 3-transitive and that the stabilizer of every three points is trivial.

2.8.5 What is the order of G when F is a finite field of order q?

2.8.6 If F is a finite field and γ is a primitive element for F, show that $AGL_1(F) = \langle t_{11}, t_{\gamma 0}\rangle$ and $G = \langle t_{11}, t_{\gamma 0}, t_{0110}\rangle$. (Recall that every finite field has a primitive element, namely, an element which generates the multiplicative group of nonzero elements of F; see for example Lang (1993) Chap. V, Sect. 5.)

2.8.7 Show that the mapping

$$\begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \mapsto t_{\alpha\beta\gamma\delta}$$

defines a homomorphism of the general linear group $GL_2(F)$ onto G whose kernel Z consists of the scalar matrices ($\alpha = \delta \neq 0$ and $\beta = \gamma = 0$). Hence $G \cong GL_2(F)/Z$. (The latter group is called the *projective general linear group* of degree 2 over F and is denoted by $PGL_2(F)$.)

2.8.8 The group $PGL_2(F)$ has a normal subgroup $PSL_2(F) = SL_2(F)Z/Z$ (the *projective special linear group*) where $SL_2(F)$ is the group of all matrices in $GL_2(F)$ with determinant 1. For which fields is it true that $PGL_2(F) = PSL_2(F)$? (The groups $PSL_2(F)$, which are sometimes denoted $L_2(F)$, are especially interesting because they are nonabelian simple groups except for the cases where $|F| = 2$ or 3.)

2.8.9 Define A to be the set of all permutations of F of the form $\xi \mapsto \xi^\sigma$ where $\sigma \in \mathrm{Aut}(F)$, the group of all field automorphisms of F. Show that A is a subgroup of $Sym(F)$ isomorphic to $\mathrm{Aut}(F)$ which normalizes both $AGL_1(F)$ and G, and that the subgroups $AGL_1(F)A$

and GA are both split extensions. (In the case when F is finite of characteristic p and order p^k, it is known that $\mathrm{Aut}(F)$ is a cyclic group of order k generated by the "Frobenius automorphism" $\xi \mapsto \xi^p$, see for example Lang (1993) Chap. V, Sect. 5.)

The higher dimensional affine and projective groups are automorphism groups of affine and projective geometries. The affine geometry $AG_d(F)$ consists of points and affine subspaces constructed from the vector space F^d of row vectors of dimension d over the field F. The points of the geometry are simply the vectors of F^d. The affine subspaces are the translates of the vector subspaces of F^d. Thus if S is a k-dimensional subspace of F^d then

$$S + \beta := \{\alpha + \beta \mid \alpha \in S\}$$

is an affine subspace of dimension k for every $\beta \in F^d$. Of course, if $\beta' \in (S + \beta)$ then $S + \beta' = S + \beta$. For example, $AG_2(\mathbb{R})$ consists of all points of $\mathbb{R}^2$ together with the straight lines in $\mathbb{R}^2$ as affine subspaces. What we have done, in fact, is neglect all metric considerations from $\mathbb{R}^2$ and retain only the incidence structure, that is, the information concerning which points are on which lines. An automorphism of the affine space $AG_d(F)$ is a permutation of the set of points which maps each affine subspace to an affine subspace (of the same dimension). In other words, an affine automorphism is a permutation of the points that preserves, or respects, the affine geometry.

An *affine transformation* is an affine automorphism of an especially simple form. For each linear transformation $a \in GL_d(F)$ and vector $v \in F^d$ we define the affine transformation $t_{a,v} : F^d \to F^d$ by

$$t_{a,v} : u \mapsto ua + v.$$

Each of these mappings $t_{a,v}$ is an automorphism of the affine geometry $AG_d(F)$. The set of all $t_{a,v}$ ($a \in GL_d(F)$, $v \in F^d$) forms the *affine group* $AGL_d(F)$ of dimension $d \geq 1$ over F. It is easy to verify that $AGL_d(F)$ is a 2-transitive subgroup of $Sym(F^d)$. The group $AGL_d(F)$ is a split extension of a regular normal subgroup T, consisting of the translations $t_{1,v}$ ($v \in F^d$), by a subgroup isomorphic to $GL_d(F)$.

Further affine automorphisms are derived from the automorphisms of the field F. For each field automorphism $\sigma \in \mathrm{Aut}(F)$ there is a permutation of F^d defined by $t_\sigma : u \mapsto u^\sigma$ where σ acts componentwise on the vector u. The mappings t_σ ($\sigma \in \mathrm{Aut}(F)$) form a subgroup of $Sym(F^d)$ isomorphic to $\mathrm{Aut}(F)$. This subgroup together with $AGL_d(F)$ generates the group $A\Gamma L_d(F)$ of *affine semilinear transformations*. The elements of $A\Gamma L_d(F)$ are precisely the permutations of F^d of the form:

$$t_{a,v,\sigma} : u \mapsto u^\sigma a + v$$

where $a \in GL_d(F)$, $v \in F^d$, and $\sigma \in \mathrm{Aut}(F)$. When $d \geq 2$, it turns out that the group $A\Gamma L_d(F)$ is the full automorphism group of the affine

geometry $AG_d(F)$ (see Exercises 2.8.10 and 2.8.12 below). In the cases where $\mathrm{Aut}(F) = 1$ (for example if $|F|$ is a prime or if $F = \mathbb{R}$ or $\mathbb{Q}$), we have $A\Gamma L_d(F) = AGL_d(F)$.

Exercises

2.8.10 Let S be a k-dimensional affine subspace in F^d. Show that S^x is an affine subspace of dimension k for each $x \in A\Gamma L_d(F)$.

2.8.11 An *affine basis* for $AG_d(F)$ is a set $B = \{\alpha_0, \dots, \alpha_d\}$ of $d+1$ points with the property that B is not contained in any $(d-1)$-dimensional affine subspace. Show that the affine group $AGL_d(F)$ acts regularly on the set of affine bases of $AG_d(F)$.

2.8.12 Let $d \geq 2$ and let $x \in Sym(F^d)$, so that x is a permutation of the points of $AG_d(F)$. Suppose that there is an integer k with $1 \leq k < d$, such that, for every k-dimensional affine subspace S of F^d, the image S^x is an affine subspace of dimension k.

(i) Show that for every ℓ with $1 \leq \ell \leq d$, x maps every ℓ-dimensional affine subspace of F^d onto an ℓ-dimensional affine subspace.

(ii) Show that for some a and v the permutation $xt_{a,v}$ fixes the origin and the d standard basis vectors $(1, \dots, 0), \cdots, (0, \dots, 1)$.

(iii) Show that the permutation $xt_{a,v}$ of part (ii) equals t_σ for some $\sigma \in \mathrm{Aut}(F)$. Deduce that $x \in A\Gamma L_d(F)$. (Note: this last part is somewhat more involved than the others. See Snapper and Troyer (1989) Prop. 84.1.)

The group $AGL_d(F)$ has several important classes of subgroups. A typical element $t_{a,v} \in AGL_d(F)$ is defined by a linear transformation $a \in GL_d(F)$ and a vector v. By insisting that the determinant of a be 1 we get the *affine special linear group*:

$$ASL_d(F) := \{t_{a,v} \in AGL_d(F) \mid \det a = 1\}.$$

Thus $ASL_d(F)$ contains the translations T as a regular normal subgroup and the stabilizer of a point is isomorphic to the special linear group $SL_d(F)$. If $d \geq 2$ then $ASL_d(F)$ acts 2-transitively on the set of points of $AG_d(F)$.

Another family of subgroups of the affine group is determined by the subfields of F. Let K be a subfield of F with finite index $k = [F : K]$. Then F is a k-dimensional vector space over K. Thus every F-vector space is also a K-vector space and any F-linear transformation is also K-linear. Specifically this means that F^d is isomorphic to K^{kd} as a K-vector space and that $GL_d(F)$ is isomorphic to a subgroup of $GL_{kd}(K)$. The translation group of an affine space is isomorphic to the additive group of the underlying vector space. Thus the identification of F^d and K^{kd} as K-vector spaces leads to an identification of the translation groups on $AG_d(F)$ and $AG_{kd}(K)$. Therefore points of the affine spaces $AG_d(F)$ and $AG_{kd}(K)$ can

be identified in such a way that the group $AGL_d(F)$ is identified with a subgroup of the affine group $AGL_{kd}(K)$. In the finite case, $AGL_m(q)$ contains a subgroup isomorphic to $AGL_r(q^s)$ whenever $m = rs$. In particular, the general linear group $GL_m(q)$ contains a subgroup isomorphic to the group $GL_1(q^m)$ which is just the (cyclic) multiplicitive group of a finite field. These subgroups are explored further in Exercises 4.6.6 and 4.6.7.

The finite affine groups $AGL_d(q)$ occupy an important position in the classification of finite primitive groups. As we shall see in Chap. 4, if G is a finite primitive group containing a regular normal abelian subgroup, then G is a subgroup of an affine group, and the regular normal subgroup of G acts as translations of the affine space. For example, if G is primitive and solvable, then it is of this form. Sect. 4.6 is devoted to the study of primitive groups with an abelian regular normal subgroup.

Exercises

2.8.13 Suppose that F is a field and that $d \geq 2$. Show that:
 (i) $ASL_d(F)$ is 2-transitive on the set of points of $AG_d(F)$.
 (ii) $ASL_d(2) = AGL_d(2)$ is 3-transitive on the set of points of $AG_d(2)$.

2.8.14 Show that for any $d \geq 1$ and any field F, the affine group $AGL_d(F)$ contains a sharply 2-transitive subgroup (that is, a subgroup H which is 2-transitive and such that $H_{\alpha\beta} = 1$ for any two points α, β).

2.8.15 Calculate the orders and indices and sketch the subgroup lattice for subgroups of the form $AGL_m(F)$ (with F a field of characteristic p) that are contained in the group $AGL_{12}(p)$ for an odd prime p. Add to your lattice the groups $ASL_m(F)$ and $A\Gamma L_m(F)$ that are contained in the group $AGL_{12}(p)$.

The *projective general linear group* $PGL_d(F)$ and *projective special linear group* $PSL_d(F)$ of dimension d over a field F are defined to be the quotient groups $GL_d(F)/Z$ and $SL_d(F)Z/Z$, respectively, where Z consists of all scalar matrices $\alpha 1$ in $GL_d(F)$. When $d = 2$, the group $PGL_d(F)$ is isomorphic to the group of linear fractional mappings (see Exercise 2.8.7). These definitions specify the projective groups as abstract groups but do not indicate a natural permutation action. For $d \geq 3$ such a natural action for the groups $PGL_d(F)$ is provided by the *projective geometry* $PG_{d-1}(F)$ of dimension $d-1$ over the field F which we describe below. We construct this geometry by using the linear action of the general linear group $GL_d(F)$.

The group $GL_d(F)$ acts on the set F^d of row vectors by right multiplication and has two orbits, namely $\{0\}$, and the set $\Omega = F^d \setminus \{0\}$ of nonzero vectors. Its action on Ω is not primitive. There is a system Λ of blocks, for $GL_d(F)$, where two vectors of Ω lie in the same block if and only if each is a scalar multiple of the other. A typical block in Λ consists of all nonzero scalar multiples of a given vector in Ω; we shall call this block a (projec-

tive) "point", and we shall use $[\alpha_1, \ldots, \alpha_d]$ to denote the point containing the nonzero vector $(\alpha_1, \ldots, \alpha_d)$. We define Λ to be the set of the points of the projective geometry $PG_{d-1}(F)$. Since Λ is a system of blocks for $GL_d(F)$, the general linear group has a permutation action on the set of projective points. The kernel of this action is the group of scalars Z, and so the image of the action on Λ is $GL_d(F)/Z = PGL_d(F)$. Thus $PGL_d(F)$ acts faithfully as a permutation group on Λ.

Define $\Delta := \{[\alpha_1, \ldots, \alpha_d] \in \Lambda \mid \alpha_d = 0\}$ (the set of "points at infinity"). Then the setwise stabilizer $G_{\{\Delta\}}$ consists of the images of those elements in $GL_d(F)$ having block matrix form

$$\begin{bmatrix} a & 0 \\ v & \alpha \end{bmatrix} \quad \text{where } a \in GL_{d-1}(F), v \in F^{d-1} \text{ and } \alpha \in F \text{ with } \alpha \neq 0.$$

If we identify the vectors in F^{d-1} with points in $PG_{d-1}(F)$ via the mapping

$$(\alpha_1, \ldots, \alpha_{d-1}) \mapsto [\alpha_1, \ldots, \alpha_{d-1}, 1]$$

then it may be verified that the setwise stabilizer $G_{\{\Delta\}}$ in its action on $\Lambda \setminus \Delta$ is permutation isomorphic to the affine group $AGL_{d-1}(F)$ acting on the set of points of $AG_{d-1}(F)$. Morover, the action induced by $G_{\{\Delta\}}$ on Δ is equivalent to the action of $PGL_{d-1}(F)$ on the the set of points of projective space $PG_{d-2}(F)$.

Exercises

2.8.16 Verify the statements of the preceding paragraph.

2.8.17 If $d > 2$, show that $PGL_d(F)$ is 2-transitive but not 3-transitive on the set of projective points points Λ.

2.8.18 Describe a typical element of the pointwise stabilizer $G_{(\Delta)}$ of the set Δ of points at infinity. Describe the action of this group on the complement of Δ.

So far we have specified the points of the projective geometry $PG_{d-1}(F)$ as the 1-dimensional vector subspaces of F^d. To complete the geometry we define the projective subspaces to be the nonzero vector subspaces of F^d. If Σ is a vector subspace of F^d, then Σ contains the 1-dimensional subspace spanned by any of its elements so Σ determines a set of projective points (by containment). The projective dimension of a projective subspace Σ is defined to be one less than its vector space dimension.

Consider, for example, the lowest dimension subspaces. Let Π denote the set of 2-dimensional subspaces of F^d. Then the elements of Π determine lines in our geometry (note how we have dropped down a dimension). A point $P \in PG_{d-1}(F)$ lies on a line $\ell \in \Pi$ when $P \subset \ell$, and a set of points is said to be "collinear" if the points are all on the same line. The automorphism group $\mathrm{Aut}(PG_{d-1}(F))$ of this geometry is the group of permutations of the points of $PG_{d-1}(F)$ which preserve the relation of collinearity. This

automorphism group acts in a natural way on the set Π of lines and also on the set of k-dimensional subspaces for any k.

In the action of $GL_d(F)$ described above it is clear that each element of $GL_d(F)$ induces an automorphism of $PG_{d-1}(F)$, and so $PGL_d(F)$ is embedded in $\mathrm{Aut}(PG_{d-1}(F))$. It is also clear that any field automorphism σ of F induces an automorphism of $PG_{d-1}(F)$ via

$$[\alpha_1, \ldots, \alpha_d] \mapsto [\alpha_1^\sigma, \ldots, \alpha_d^\sigma].$$

The group generated by these two types of automorphisms is called the *projective semilinear group* and is denoted $P\Gamma L_d(F)$. One can show that $P\Gamma L_d(F)$ is the full automorphism group of $PG_{d-1}(F)$ for $d \geq 3$ (see for example Artin (1988) Theorem 2.26 or Samuel (1988) Theorem 7).

Exercises

2.8.19 A set of $d+1$ points in $PG_{d-1}(F)$ is a *basis* if no subset of d of the points is contained in a projective subspace of dimension $d-2$. Show that the group $PGL_d(F)$ acts regularly on the set of bases of PG_{d-1}. (This is one modern form of the "Fundamental Theorem of Projective Geometry".)

2.8.20 Let x be a permutation of the set of points of $PG_d(F)$. If x preserves collinearity, show it must also map each projective subspace to a projective subspace of the same dimension.

2.8.21 Show that $SL_d(F)$ acts transitively on the set Π of projective lines and also on the set of all triangles (that is, triples of non-collinear points) in $PG_{d-1}(F)$ (for $d \geq 3$). In particular the group $PSL_d(F)$ is 2-transitive on the points of $PG_{d-1}(F)$.

2.8.22 Show how to identify the Fano plane (Exercise 2.4.2) with $PG_2(2)$. Hence show that the automorphism group of the Fano plane is isomorphic to $PGL_3(2) = PSL_3(2)$.

2.8.23 Suppose that F is a finite field of order q.
  (i) Show that $PG_{d-1}(q)$ has $(q^d-1)/(q-1)$ points.
  (ii) Show that $PG_{d-1}(q)$ has $|\Pi| = (q^d-1)(q^{d-1}-1)/(q^2-1)(q-1)$ lines.
  (iii) Deduce that $PGL_3(q)$ has two subgroups of index q^2+q+1 which are not conjugate.

2.8.24 Consider the projective plane $PG_2(F)$. Show that any two points lie on a unique line and any two lines intersect in a unique point. In particular, the theory of projective planes lacks any concept of parallel lines.

2.9 The Transitive Groups of Degree at Most 7

In the preceding sections we have discussed a variety of constructions for permutation groups. We shall now apply these ideas to give a census of

transitive groups of small degrees up to permutation isomorphism. In each case we leave aside the alternating and symmetric groups of the given degree as "improper" groups.

There are no proper transitive subgroups of S_n for $n \leq 3$, and for $n = 4$ it is a simple exercise to show that up to permutation isomorphism (that is, conjugacy in S_n) there are only three: the cyclic group $\langle(1234)\rangle$, the non-cyclic group $\langle(12)(34), (13)(24)\rangle$ and the Sylow 2-subgroup $\langle(1234), (13)\rangle$. In discussing the case $n = 5$ we shall find the following lemma useful.

Lemma 2.9A. *Let $n \geq 5$. If $G \leq S_n$ and $G \neq A_n$ or S_n, then $|S_n : G| \geq n$.*

PROOF. The proof depends on a result which we shall prove in Chap. 3 (see Corollary 3.3A) namely, that when $n \geq 5$ the only normal subgroups of S_n are 1, A_n and S_n. Now, Example 1.3.4 shows that there is a representation of S_n as a transitive group of degree $d := |S_n : G|$ acting on the set of right cosets of G in S_n, and that the kernel of the representation is contained in G. Since G does not contain A_n, we conclude that the representation is faithful, and so S_n is isomorphic to a subgroup of S_d. Hence $d \geq n$ as asserted. □

Now consider a "proper" transitive subgroup G of S_5. Then the index of a point stabilizer of G in G is 5, so $|G| = 5k$ for some integer k. By Lemma 2.9A, $5k \leq 120/5$ and so $k \leq 4$. Thus by the Sylow theorems (see Exercise 1.4.13) we conclude that there is a unique (normal) Sylow 5-subgroup P of G of order 5. Without loss in generality we may take $P = \langle(12345)\rangle$. It is now easy to show that the normalizer of P in S_5 is $N := \langle P, (2354)\rangle$ which has order 20, and so there are just three possible choices for G (of orders 5,10 and 20, respectively).

Exercises

2.9.1 Check that every proper transitive subgroup of S_4 is conjugate to one of the three groups listed above.

2.9.2 Show that the normalizer N of the cyclic subgroup $C := \langle(12\ldots n)\rangle$ in S_n is a split extension of C by

$$H := \{u_k \in S_n \mid 1 \leq k \leq n \text{ and } \mathrm{GCD}(k, n) = 1\}$$

where $u_k : i \mapsto ki \bmod n$. ($\mathrm{GCD}(k, n)$ denotes the greatest common divisor of k and n.)

2.9.3 Verify that each proper transitive subgroup of S_5 is conjugate to one of the three groups just described.

We now turn to the transitive groups of degree 6. In this case the enumeration is considerably more challenging since up to permutation isomorphism there are 14 proper transitive groups of this degree (given in Table 2.1) in addition to the two improper groups A_6 and S_6. We shall describe each of

TABLE 2.1. The Proper Transitive Groups of Degrees 4, 5, 6 and 7

	Order	Description	Generators
Degree 4			
T4.1	4	C_4	(1234)
T4.2	4	$C_2 \times C_2$	(12)(34), (13)(24)
T4.3	8	$C_2\ wr_2\ C_2$	(1234), (12)
Degree 5			
T5.1	5	C_5	(12345)
T5.2	10	$ASL_1(5)$	(12345), (25)(34)
T5.3	20	$AGL_1(5)$	(12345), (2354)
Degree 6			
T6.1	6	C_6	(123456)
T6.2	6	S_3	(12)(34)(56), (135)(246)
T6.3	12	D_{12}	(123456), (16)(25)(34)
T6.4	48	$S_2\ wr_3\ S_3$	(123)(456), (12)(45)(14)
T6.5	24	$A_6 \cap$ T6.4	(123)(456), (12)(45), (14)(25)
T6.6	24	S_4	(123)(456), (1542)
T6.7	12	$A_6 \cap$ T6.6	(123)(456), (14)(25)
T6.8	24	$C_2\ wr_3\ C_3$	(123)(456), (14)
T6.9	72	$S_3\ wr_2\ C_2$	(123), (12), (14)(25)(36)
T6.10	36	$A_6 \cap$ T6.9	(123), (1542)(36)
T6.11	36	$3^2 \cdot 2^2$	(123), (12)(45), (14)(25)(36)
T6.12	18	$C_3\ wr_2\ C_2$	(123), (14)(25)(36)
T6.13	120	$PGL_2(5)$	(01234), (0∞)(14)(1243)
T6.14	60	$PSL_2(5)$	(01234), (0∞)(14)
Degree 7			
T7.1	7	C_7	(1234567)
T7.2	14	$C_7 \cdot 2$	(1234567), (27)(36)(45)
T7.3	21	$ASL_1(7)$	(1234567), (235)(476)
T7.4	42	$AGL_1(7)$	(1234567), (243756)
T7.5	168	$PGL_3(2)$	(1234567), (23)(47)

these groups and then at the end give some indication how to check that we have a full list.

First of all there are the regular groups. These correspond to the regular representations of the groups of order 6, so there are two of them: a cyclic group and a group isomorphic to S_3 (T6.1 and T6.2 in the table). Next there is a variety of groups which we can obtain by the constructions described earlier in this chapter.

Since the binomial coefficient $\binom{4}{2} = 6$, the action of S_4 on 2-sets has degree 6 (see Example 2.1.2). Relabelling the points gives an imprimitive

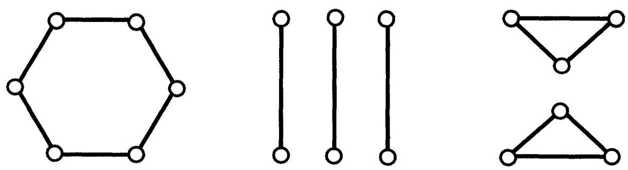
subgroup of order 24 in S_6 (T6.6). It can be seen that this group has blocks of size 2, and its action on a system of these blocks is like the symmetric group of degree 3. The even permutations in the subgroup T6.6 form another transitive group T6.7 of order 12.

Transitive groups of degree 6 also arise as automorphism groups of sufficiently symmetric structures, in particular, of suitable graphs. In order that the automorphism group of a graph should be transitive (on the set of vertices) it is certainly necessary for each vertex to have the same degree. It can be verified that the automorphism groups of each of the graphs in Fig. 2.5 is indeed transitive.

Exercise

2.9.4 Show that these are the only graphs with six vertices and transitive automorphism groups in which each vertex has degree 1 or 2. Explain why, for our purposes, it is enough to look at graphs where the common degree of the vertices is at most half the number of vertices.

In the case of the first graph we find that the automorphism group is the dihedral group $\langle x, y\rangle$ of order 12 where $x = (123456), y = (16)(25)(34)$ and $y^{-1}xy = x^{-1}$ (T6.3); it contains T6.1 and has blocks both of size 2 and size 3. The automorphism group of the second graph is generated by $(123)(456), (12)(45)$ and (14) (T6.4). The stabilizer of 1 is easily seen to be of order 8 and so the group has order $6 \cdot 8 = 48$ by the orbit-stabilizer property. The sets $\{1,4\}, \{2,5\}$ and $\{3,6\}$ form a system of blocks and since $|S_2\ wr_3\ S_3| = 2^3 6 = 48$ (with the natural action of S_3), we conclude that T6.4 is permutation isomorphic to $S_2\ wr_3\ S_3$ (see Exercise 2.6.2). The even permutations in the group T6.4 constitute a proper transitive subgroup T6.5. The group T6.4 also contains another transitive subgroup, T6.8, of order $2^3 \cdot 3 = 24$ obtained by replacing the group S_3 in $S_2\ wr_3\ S_3$ by its cyclic subgroup of order 3; T6.8 can be generated by $(123)(456)$ and (14).



(a) (b) (c)

FIGURE 2.5.

Exercise

2.9.5 All the groups T6.5, T6.6 and T6.8 are imprimitive groups of order 24 and degree 6 with blocks of size 2. However, show that they are not permutation isomorphic.

The automorphism group of the third graph is generated by (123), (12) and (14)(25)(36), and can be seen to be permutation isomorphic to $S_3\ wr_2\ S_2$ with the natural action of S_2 (T6.9). It therefore has order $6^2 \cdot 2 = 72$. Moreover, group T6.9 has two nonisomorphic transitive subgroups of index 2 and order 36, namely, the group T6.10 of all even permutations in T6.9, and the group T6.11 generated by the elements (123), (12)(45) and (14)(25)(36). The latter subgroup also contains a transitive subgroup T6.12 generated by (123) and (14)(25)(36) which is isomorphic to a subgroup of the wreath product $S_3\ wr_2\ S_2$ where S_3 is replaced by a cyclic group of order 3. This latter group is also the automorphism group of the digraph obtained by modifying the graph so that each of the triangles is a directed cycle.

The remaining proper transitive groups of degree 6 are primitive groups, namely the projective linear groups $PGL_2(5)$ and $PSL_2(5)$ of orders 120 and 60 respectively (see Sect. 2.8). These groups appear as T6.13 and T6.14 in the table, and in terms of their natural symbols 0,1,2,3,4 and ∞ these groups can be generated by the functions: $\xi \mapsto \xi + 1, \xi \mapsto 1/\xi$ and $\xi \mapsto 2\xi$; and $\xi \mapsto \xi + 1, \xi \mapsto 1/\xi$ and $\xi \mapsto -\xi$, respectively.

This completes the list of the 14 proper transitive groups of degree 6. We shall not prove that these are indeed the only groups, but in Exercise 2.9.8 we shall give an indication how one might try to do this. While this case study is an illuminating exercise, it should be realized that degree 6 is too small to be generic, and the list is rather atypical. For example, in our list the largest imprimitive group T6.9 is small compared with primitive group T6.13. As we shall see later (Chap. 5), this can only happen for small degrees; for larger degrees, the proper primitive groups have very small orders compared to the largest imprimitive groups.

Table 2.1 also lists the five proper transitive groups of degree 7. These are simpler to obtain and are left as an exercise.

Exercises

2.9.6 Identify the transitive groups from the table which are isomorphic to the images of the following actions of the symmetry group G of the cube:
   (i) The action of G on the set of six faces of the cube;
   (ii) The action of G on the set of six pairs of opposite edges (this action is not faithful);
   (iii) The action of the subgroup of the rotations in G on the faces.

2.9.7 Identify the following transitive groups among those in the table:
   (i) The automorphism group of the graph in Fig. 2.6.

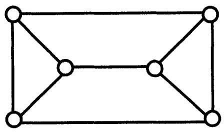


FIGURE 2.6.

(ii) The permutation group induced by the symmetry group of the icosahedron on the set of six pairs of opposite vertices.

2.9.8 Let G be a proper transitive subgroup of S_6. Prove:

(i) If G contains a 5-cycle, then G is 2-transitive and has order 60 or 120;

(ii) If G contains a 3-cycle but no 5-cycle, then the support of the 3-cycle is a block for G;

(iii) If G contains no 3- or 5-cycle, then its point stabilizer is a 2-group and G has a block of size 2.

(This exercise is a first step in showing that the groups in our table form a complete list. In particular, it shows that either G is primitive of order 60 or 120, or G is imprimitive. In the latter case G is permutation isomorphic to a subgroup of $S_3\ wr_2\ S_2$ or of $S_2\ wr_3\ S_3$, so this case requires an analysis of the transitive subgroups of these latter groups.)

2.9.9 Prove that $PSL_2(5) \cong A_5$. [*Hint:* Find a permutation representation of degree 5 of the former group.]

2.9.10 Show that $PGL_2(5) \not\cong S_5$.

2.9.11 Verify that Table 2.1 gives all the proper transitive permutation groups of degree 7.

2.10 Notes

- Exercise 2.2.8: A lot is known about automorphism groups of ordered sets; see, for example, Droste (1985) and references there. For related results see Lauchli and Neumann (1988).
- Exercise 2.3.10: Cayley graphs were introduced as "colour graphs" by A. Cayley in 1878; see Burnside (1911) §304 for further historical details.
- Exercise 2.3.11: See Sect. 9.2 for related results.
- Exercise 2.4.5: See Wielandt (1969). See also Liebeck et al. (1988b).
- Exercises 2.4.7–10: See Maurer (1955) and Karrass and Solitar (1956). Completeness of (S, d) as a metric space permits use of the Baire category theorem; see, for example, Cameron (1990) Sect. 2.4 and Dixon (1990).
- Sects. 2.6 and 2.7: Various forms of the wreath product construction are quite old, going back at least to G. Frobenius at the end of the 19th

century (as groups of "monomial matrices"). The name appears to have been introduced by G. Pólya in the 1930s and became standard terminology in the 1950s. A general wreath product construction (called the "complete product") was introduced in a series of papers by L. Kaloujnine and M. Krasner around 1948; see below for specific references. See also P. Hall (1962).

- Theorem 2.6A: See Kaloujnine and Krasner (1948).
- Example 2.6.1: See Kaloujnine (1948); P.M. Neumann informs us that a similar construction appears in a paper of Cauchy. For related results, see Berkovic (1989).
- Lemma 2.7A: Part of the "folk-lore", and stated without proof in Cameron (1981a). According to P.M. Neumann, a special case was proved by W. Manning at the beginning of this century.
- Exercise 2.7.3: See Seager (1988).
- Sect. 2.8: For general reference to the affine and projective groups see, for example, Artin (1957) or Snapper and Troyer (1971).
- Sect. 2.9: At the end of the 19th century many papers were published, notably by F.N. Cole and G.A. Miller, enumerating the permutation groups of small degrees. These include a not quite correct list of Miller listing over 300 transitive groups of degree 12. See also Burnside (1911) §166 (which mistakenly includes some groups of degree 8 which are not primitive). More reliable lists of primitive and transitive groups (giving generators and structural information) have appeared since, including Sims (1970) (primitive groups of degree ≤ 20), Butler and McKay (1983) (transitive groups of degree ≤ 11), and Short (1992) (solvable primitive groups of degree less than 256). Although these lists have been extended [for example, Royle (1987)], they soon become quite unwieldy to use by hand; the libraries of primitive and transitive groups in the computer algebra systems MAGMA and GAP now provide the most reliable and extensive sources. In Appendix B we give a summary list of the primitive groups of degree < 1000.

3

The Action of a Permutation Group

3.1 Introduction

The next three chapters are primarily devoted to studying primitive groups. Primitive groups play an important role as building blocks, particularly in the study of finite permutation groups. Frequently, we can carry out a series of reductions: from the general case to the transitive case by examining the action of the group on its orbits and its point stabilizers, and then from the transitive imprimitive case to the primitive case by studying the action of the group on sets of blocks and the block stabilizers. Eventually, at least for finite permutation groups, this reduces the original question to one about primitive groups. Of course, this is rarely the whole problem; generally we must then retrace the process, fitting the information back together as we reconstruct the original group, and often this is very complicated. Still, the crux of many problems in finite permutation groups lies in the study of the primitive case.

A large part of this chapter develops combinatorial methods to study the action of the point stabilizer of a transitive group, methods which are especially effective for primitive groups. In Chap. 4 we apply more direct group theoretic methods which enable us to describe the subgroup structure of finite primitive groups in greater detail. These latter methods have turned out to be very powerful when combined with the classification of finite simple groups. In Chap. 5, combinatorial techniques are used to give bounds on the orders of primitive groups.

Any subgroup of $Sym(\Omega)$ which contains $Alt(\Omega)$ is primitive (provided $|\Omega| > 2$), but such a subgroup is quite atypical as a primitive group; we call such subgroups *improper* primitive groups. The remaining primitive subgroups of $Sym(\Omega)$ are called *proper*, and it is these in which we are interested. Typically, as we shall see in Theorem 3.3B and Chap. 5, the proper primitive groups have very small orders compared with the order of the symmetric group. They are also quite rare. As Table 3.1 suggests, the number $P(n)$ of proper permutation groups of degree n (up to permutation isomorphism) grows slowly and irregularly. Indeed, it is a consequence of the

TABLE 3.1. Number of Proper Primitive Groups of Degree n

$n =$	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$P(n) =$	3	2	5	5	9	7	6	4	7	2	4	20	8	2	6	2

classification of finite simple groups that there are infinitely many values of n (namely, $n = 3, 4, 34, 39, 46, \ldots$) for which $P(n) = 0$; for these degrees, only the alternating and symmetric groups are primitive [see Cameron et al. (1982)]. A complete list of primitive groups of degree less than 1000 is given in Appendix B.

The following example is a typical illustration of the relative sizes of the intransitive, imprimitive and proper primitive subgroups of the symmetric group (see Sect. 5.2). In S_{16}, the largest intransitive subgroup has index 16, and the next largest has index 120. On the other hand, the largest imprimitive subgroup of S_{16} has index 6435, and the largest proper primitive subgroup has index 64864800.

Exercise

3.1.1 Construct the subgroups of S_{16} referred to in the last paragraph. [*Hint:* The first two are stabilizers of a point and of a 2-element subset. The largest imprimitive subgroup has blocks of size 8, and the primitive subgroup is permutation isomorphic to $AGL_2(4)$.]

3.2 Orbits of the Stabilizer

As we saw earlier (see Sect. 2.3), graphs and digraphs can often be used to define interesting groups. As a first step in our analysis of primitive groups we shall show how an arbitrary transitive permutation group can be seen to act as a group of automorphisms of a digraph.

Throughout this section G will denote a group acting transitively on a set Ω. For such a group we can construct a natural family of digraphs on which G acts (preserving the incidence structures). We begin with the usual action of G on the cartesian product $\Omega \times \Omega$. The orbits of G on this set are called the *orbitals* of G on Ω. The least interesting of these is the orbital $\Delta_1 := \{(\alpha, \alpha) \mid \alpha \in \Omega\}$; the other orbitals are called . For each orbital Δ there is an orbital, denoted Δ^*, where $(\alpha, \beta) \in \Delta^*$ if and only $(\beta, \alpha) \in \Delta$. Clearly, $(\Delta^*)^* = \Delta$. An orbital is *self-paired* if $\Delta^* = \Delta$; for example, the diagonal orbital is self-paired.

Now for each orbital Δ of G we define the digraph Graph(Δ) with vertex set Ω and edge set Δ. For the diagonal orbital Δ_1, the Graph(Δ_1) is just a digraph with a loop at each vertex, but for the other orbitals Graph(Δ) is a digraph without loops. The digraph Graph(Δ^*) for the paired orbital

is obtained from Graph(Δ) by reversing the directions of the edges, and Δ is self-paired if and only if the digraph Graph(Δ) is a graph. Because Δ is G-invariant, G acts on Graph(Δ) preserving the adjacency structure. The simple exercises below illustrate these concepts.

Exercises

3.2.1 Consider the two groups $H = \langle(12345)\rangle$ and $K = \langle(12345), (25)(34)\rangle$. Sketch the digraphs for the four nondiagonal orbitals of H and for the two nondiagonal orbitals of K.

3.2.2 The symmetry group of the cube acting on the set of 8 vertices (see Example 1.4.1) has three nondiagonal orbitals. Sketch the corresponding digraphs.

3.2.3 Consider the group A of automorphisms of the infinite trivalent tree $\mathcal{T}$ described in Example 1.5.4. Let $d(\alpha, \beta)$ denote the distance in $\mathcal{T}$ between two vertices α and β. Show that the set $\Delta_k := \{(\alpha, \beta) \mid d(\alpha, \beta) = k\}$ is an orbital for each $k \geq 0$.

3.2.4 Consider the action of degree 10 of S_5 on the set of 2-subsets of $\{1, 2, 3, 4, 5\}$. Show that there are three orbitals and sketch the digraphs for the two nondiagonal orbitals. Do these digraphs look familiar?

3.2.5 Show that an orbital Δ for a transitive group G is self-paired if and only if there exists $(\alpha, \beta) \in \Delta$ and $x \in G$ such that x interchanges α and β. If G is finite, show that every nondiagonal self-paired orbital has even length, and show that G has odd order if and only if no nondiagonal orbital is self-paired.

There is a close relationship between the orbitals of G and the orbits of the point stabilizers of G. Recall that, since we are assuming that G acts transitively on Ω, the point stabilizers are conjugate in G by Corollary 1.4A. For each orbital Δ of G and each $\alpha \in \Omega$, we define

$$\Delta(\alpha) := \{\beta \in \Omega \mid (\alpha, \beta) \in \Delta\}$$

which is the set of vertices in Graph(Δ) which lie on an edge from α. It is now easy to verify that the mapping $\Delta \mapsto \Delta(\alpha)$ is a bijection from the set of orbitals of G onto the set of orbits of G_α with the diagonal orbital mapping onto the trivial orbit $\{\alpha\}$. In particular, the number of orbitals is equal to the number of orbits of G_α; this number is called the *rank* of G. An orbit of G_α for any $\alpha \in \Omega$ is called a *suborbit* of G, and if Δ and Δ^* are paired orbitals, then $\Delta(\alpha)$ and $\Delta^*(\alpha)$ are called *paired suborbits.* Note that if $x \in G$ and $\alpha^x = \beta$, then $\Delta(\alpha)^x = \Delta(\beta)$, which gives a canonical mapping from the set of orbits of G_α onto the set of orbits for G_β, that is, $\Delta(\beta)$ is independent of the choice of x.

Exercises

3.2.6 Verify the statements in the preceding paragraph.

3.2.7 Assuming that G is transitive on Ω, show that $|\Delta(\alpha)|\,|\Omega| = |\Delta|$ for each orbital Δ. In particular, $|\Delta(\alpha)| = |\Delta^*(\alpha)|$ if Ω is finite.

3.2.8 Let $\Omega = \mathbb{F}_q$ be the finite field with q elements and suppose that q is odd. Let G be the group of all permutations of the form $\xi \mapsto \alpha\xi + \beta$ with $\alpha, \beta \in \mathbb{F}_q$ where α is a nonzero square in $\mathbb{F}_q$. Show that G has two nondiagonal orbitals of the same size. Are they paired?

3.2.9 Let $G = AGL_1(\mathbb{Q})$ and $t \in G$ be defined by $t : \xi \to \xi + 1$. Consider the action of G by right multiplication on the set Γ_H of right cosets of $H := \langle T \rangle$ in G. Show that G has paired suborbits of different sizes (contrast with Exercise 3.2.7).

3.2.10 Consider the action of $SL_2(\mathbb{Q})$ by right multiplication on the set of right cosets of the subgroup $SL_2(\mathbb{Z})$ in $SL_2(\mathbb{Q})$. Show that each suborbit in this action is finite. Is the action primitive?

3.2.11 Let G be a transitive permutation group of degree n where n is odd. Show that G has odd order if and only if each suborbit has odd length.

We now show how to characterize primitivity in terms of the digraphs Graph(Δ). In general, let $\mathcal{G}$ be a digraph. A sequence $v_0, v_1, \ldots, v_m$ of vertices is called a *directed path* of *length* m from v_0 to v_m if there is an edge in $\mathcal{G}$ from v_i to v_{i+1} for $i = 0, \ldots, m-1$. The sequence is called an *undirected path* if, for each i, there is an edge from v_i to v_{i+1} or an edge from v_{i+1} to v_i. We say that $\mathcal{G}$ is *connected* if for every pair of vertices u and v there is an undirected path from u to v, and $\mathcal{G}$ is *strongly connected* if this path can always be chosen to be directed.

EXAMPLE 3.2.1. Let $G = \langle x \rangle$ be an infinite cyclic group acting on $\mathbb{Z}$ by $\alpha^x := \alpha + 1$. Then $\Delta := \{(\alpha, \alpha+1) \mid \alpha \in \mathbb{Z}\}$ is an orbital for G, and Graph(Δ) has the form:

$$\cdots \longrightarrow -1 \longrightarrow 0 \longrightarrow 1 \longrightarrow 2 \longrightarrow \cdots$$

This digraph is connected, but not strongly connected.

The following theorem gives another characterization of primitivity.

Theorem 3.2A. *Let G be a group acting transitively on a set Ω. Then G acts primitively if and only if Graph(Δ) is connected for each nondiagonal orbital Δ.*

PROOF. First suppose that Graph(Δ) is connected for each nondiagonal orbital of G. Let $\Gamma \subseteq \Omega$ be a block for G containing at least two points, say α and β. Let Δ be the orbital for G containing (α, β). We want to show that $\gamma \in \Gamma$ for each $\gamma \in \Omega$. Indeed, since Graph(Δ) is connected, there is an undirected path $\alpha = \alpha_0, \ldots, \alpha_k = \gamma$ in Graph(Δ), and we shall show by induction that $\alpha_i \in \Gamma$ for $i = 0, 1, \ldots k$. This is true for $i = 0$, so suppose $i > 0$ and that $\alpha_{i-1} \in \Gamma$. Since $(\alpha_{i-1}, \alpha_i) \in \Delta \cup \Delta^*$, there exists

$x \in G$ such that $(\alpha^x, \beta^x) = (\alpha_{i-1}, \alpha_i)$ or (α_i, α_{i-1}). Because Γ is a block and contains either α^x or β^x, therefore $\Gamma = \Gamma^x$ and so $\alpha_i \in \Gamma$. This proves the induction step, and we conclude that $\gamma \in \Gamma$ for each γ in Ω. Hence G has no proper blocks and so is primitive.

Conversely, suppose that there is a nondiagonal orbital Δ such that Graph(Δ) is not connected. Consider the relation $\equiv$ defined on Ω by: $\alpha \equiv \beta \iff$ there exists an undirected path from α to β in Graph(Δ). This is easily seen to be a G-congruence (see Exercise 1.5.4), which is proper since Graph(Δ) is not connected. Hence G is not primitive. □

In general, the graphs Graph(Δ) in Theorem 3.2A are not *strongly* connected. We shall say that a group acting transitively on Ω is *strongly primitive* if the orbital graphs Graph(Δ) are strongly connected for each nondiagonal orbital Δ. Theorem 3.2A shows that a strongly primitive group is certainly primitive, but the following example shows that the converse is not true.

EXAMPLE 3.2.2. Let $G := \mathrm{Aut}(\mathbb{Q}, \leq)$ be the group of permutations of $\mathbb{Q}$ which preserve the usual ordering $\leq$ (see Exercise 2.2.8). Then G has two nondiagonal orbitals, namely, $\Delta := \{(\alpha, \beta) \in \mathbb{Q}^{(2)} \mid \alpha < \beta\}$ and its paired orbital Δ^*. Clearly, Graph(Δ) and Graph(Δ^*) are both connected, but are not strongly connected. Hence G is primitive, but not strongly primitive.

The following lemma gives criteria for a primitive group to be strongly primitive. In particular, it shows that for finite groups "primitivity" and "strong primitivity" are equivalent. Another criterion for strong primitivity is given in Exercise 3.2.12.

Lemma 3.2A. *Let G be a group acting primitively on Ω.*

(i) *Graph(Δ) is strongly connected for a nondiagonal orbit Δ of G $\iff$ Graph(Δ) contains a nontrivial directed cycle (that is, a directed path $\alpha_0, \alpha_1, \ldots \alpha_m$ in Graph(Δ) with $\alpha_0 = \alpha_m$ and $m > 1$).*

(ii) *If for each pair of distinct points α and β there exists $z \in G$ with a cycle of finite length containing both α and β, then G is strongly primitive.*

(iii) *If G is periodic (in particular, if G is finite), then G is strongly primitive.*

Remark. Part (i) of the lemma can also be interpreted as saying that Graph(Δ) is *not* strongly connected if and only if the (G-invariant) relation ρ on Ω given by:

$$\alpha\rho\beta \Leftrightarrow \text{there is a directed path in Graph}(\Delta) \text{ from } \alpha \text{ to } \beta$$

is a partial ordering.

PROOF. (i) It is clear that Graph(Δ) is strongly connected if and only if every pair of distinct points lie on a directed cycle, so one implication is trivial. On the other hand, suppose that Graph(Δ) contains at least one nontrivial cycle. Consider the binary relation $\equiv$ on Ω given by: $\alpha \equiv \beta \iff \alpha = \beta$ or α and β lie on a nontrivial directed circuit in Graph(Δ). This is easily seen to be a G-congruence on Ω and, because G acts primitively, the congruence classes must be either singletons or Ω itself (see Exercise 1.5.4). Since Graph(Δ) contains a nontrivial directed cycle, the congruence classes cannot all be singletons, and so $\alpha \equiv \beta$ for all α and β. Hence Graph(Δ) is strongly connected as required.

(ii) We have to show that Graph(Δ) is strongly connected for each nondiagonal orbit Δ. Choose $(\alpha, \beta) \in \Delta$, and $z \in G$ such that z has a cycle of finite length containing α and β. Then some power y of z maps α onto β, and y^m fixes α for some $m > 1$. Thus $\alpha, \beta = \alpha^y, \alpha^{y^2}, \dots, \alpha^{y^m} = \alpha$ is a nontrivial directed cycle in Graph(Δ), and so Graph(Δ) is strongly connected by (i).

(iii) Follows immediately from (ii) (we can choose z so that $\alpha^z = \beta$ because G is transitive). □

Exercises

3.2.12 Suppose that the group G acts transitively on Ω and let G_α be a point stabilizer. Show that G is strongly primitive if and only if there is no subset T with the properties $G_\alpha \subset T \subset G$ and $TT \subseteq T$ (in other words, G_α is a maximal subsemigroup of G). (Compare with Lemma 1.5A.)

3.2.13 Let G be a finite primitive group with a suborbit of length 2. Show that G is finite, that each point stabilizer has order 2, and that G has prime degree. Hence show that G is a dihedral group. [*Hint:* Look at the digraph for the corresponding orbital.]

3.2.14 Use Theorem 3.2A and Lemma 3.2A to describe an algorithm which you could use to decide whether a finite permutation group is primitive (assume that the group is defined by a set of generating permutations). What information can you get about blocks in the case that Graph(Δ) is not connected for some nondiagonal orbital Δ? (See Sect. 3.6.)

Theorem 3.2A uses each of the orbitals separately, but we can obtain more powerful results by combining the orbitals and the digraphs Graph(Δ). We define the *colour graph* $\mathcal{G}$ of the transitive group G to be a labeled digraph with vertex set Ω and full edge set $\Omega \times \Omega$ where each edge (α, β) is labeled with a "colour" identifying the orbital from which it comes. Clearly G acts on the set of vertices of $\mathcal{G}$ in such a way as to preserve the colours of all the edges. This leads us to introduce a binary

operation $\circ$ on the set of all sets of edges of $\mathcal{G}$. Let $\Sigma, \Gamma \subseteq \Omega \times \Omega$, then

$$\Sigma \circ \Gamma := \{(\alpha, \beta) \mid (\alpha, \gamma) \in \Sigma \text{ and } (\gamma, \beta) \in \Gamma \text{ for some } \gamma \in \Omega\}.$$

Thus $\Sigma \circ \Gamma$ is the set of all edges (α, β) in $\mathcal{G}$ such that there is a path of length 2 from α to β whose edges are from Σ and Γ, respectively. The operation $\circ$ is associative, and we can define "powers" by

$$\Sigma^{(0)} := \Delta_1 \text{ (the diagonal orbital)} \quad \text{and} \quad \Sigma^{(k)} := \Sigma \circ \Sigma^{(k-1)} \quad \text{for } k \geq 1.$$

Also, for any set Σ of edges and any $\alpha \in \Omega$, we shall write

$$\Sigma(\alpha) := \{\beta \in \Omega \mid (\alpha, \beta) \in \Sigma\}$$

and so $\Sigma(\alpha)$ consists of all heads of directed edges in Σ with their tails at α. These constructions are applied in the next theorem.

Theorem 3.2B. *Let G be a group acting transitively on the set Ω.*

(i) *Let Σ and Λ be subsets of $\Omega \times \Omega$, and suppose that Λ is G-invariant. Then $|\Sigma \circ \Lambda(\alpha)| \leq |\Sigma(\alpha)|\,|\Lambda(\alpha)|$ for all $\alpha \in \Omega$.*

(ii) *Suppose that G is primitive and Δ is a nondiagonal orbital for G, and put $\Gamma := \Delta \cup \Delta^*$. Then $\bigcup_{k \geq 0} \Gamma^{(k)} = \Omega \times \Omega$; and, if G has finite rank r, then it is sufficient to take the union over all $k \leq r-1$. Moreover, if Graph(Δ) is strongly connected, then the same conclusion holds with Γ replaced by Δ.*

(iii) *If G is primitive with finite rank r and some suborbit has finite length $m > 1$, then Ω is finite and $|\Omega| \leq 1 + m + \cdots + m^{r-1}$.*

PROOF. (i) Clearly, $(\Sigma \circ \Lambda)(\alpha) = \bigcup_{\gamma \in \Sigma(\alpha)} \Lambda(\gamma)$. On the other hand, for all $x \in G, \Lambda(\alpha)^x = \Lambda(\alpha^x)$ because Λ is G-invariant, and so $|\Lambda(\gamma)| = |\Lambda(\alpha)|$ for all $\gamma \in \Omega$ by the transitivity of G. The result now follows.

(ii) Since $(\alpha, \beta) \in \Gamma^{(k)} \iff$ there is a nondirected path of length k from α to β in Graph(Δ), the first assertion of (ii) follows at once from Theorem 3.2A. Now define $\Phi(s) := \bigcup_{0 \leq k \leq s} \Gamma^{(k)}$ and consider the chain of subsets $\Phi(0) \subseteq \Phi(1) \subseteq \Phi(2) \subseteq \ldots$. If $\Phi(t) = \Phi(t-1)$ for some $t \geq 1$, then $\Gamma^{(t+1)} \subseteq \Phi(t-1) \circ \Gamma \subseteq \Phi(t)$, and so $\Phi(t+1) = \Phi(t)$. Hence, by induction, we have $\Phi(s) = \Phi(t-1)$ for all $s \geq t$ and so $\Phi(t-1) = \Omega \times \Omega$. On the other hand, each orbital of G is contained in some $\Delta^{(k)}$ because the latter are G-invariant sets whose union is $\Omega \times \Omega$ and the former is an orbit for G on this set. Thus, if G has rank r, then at most r of the sets $\Phi(s)$ can differ from one another. In particular, $\Phi(r-1) = \Omega \times \Omega$ as asserted. A similar argument applies (with Γ replaced by Δ) in the case where Graph(Δ) is strongly connected.

(iii) Let Δ be an orbital for G with $|\Delta(\alpha)| = m$; since $m > 1, \Delta$ is nondiagonal. We shall first show that Graph(Δ) must be strongly connected. Indeed, for each $\alpha \in \Omega$, define $\Omega[\alpha]$ to be the set of all $\gamma \in \Omega$ for which there is a directed path in Graph(Δ) from α to γ. The argument in (ii) above

shows that $\Omega[\alpha] = \bigcup_{0\leq k<r} \Delta^{(k)}(\alpha)$, and so $\Omega[\alpha]$ is finite by the finiteness of $\Delta(\alpha)$. Since $\Omega[\alpha]^x = \Omega[\alpha^x]$, the transitivity of G shows that $|\Omega[\alpha]|$ is independent of α, while $|\Omega[\alpha]| > 1$ because $|\Delta(\alpha)| > 1$. Choose $\beta \neq \alpha$ in $\Omega[\alpha]$, and note that $\Omega[\beta] \subseteq \Omega[\alpha]$ by the definition of $\Omega[\alpha]$. Since the two sets have the same finite size, therefore $\Omega[\alpha] = \Omega[\beta]$. Thus $\alpha \in \Omega[\beta]$ and $\beta \in \Omega[\alpha]$, so there is a directed cycle in Graph(Δ) passing through α and β. Hence Graph(Δ) is strongly connected by Lemma 3.2$A(i)$.

Finally (ii) applies to conclude that $\Omega[\alpha] = \Omega$, and so $|\Omega| \leq \sum_{0\leq k<r} \left|\Delta^{(k)}(\alpha)\right| \leq 1 + m + \cdots + m^{r-1}$ by (i). □

In the case of a finite transitive permutation group G of degree n, the list of *subdegrees* (the lengths of the orbits of one of the point stabilizers) is an invariant of G. We shall denote them in increasing order: $n_1 = 1, n_2, \ldots, n_r$ where r is the rank of G. Note that, if G is primitive and not regular of prime degree, then $n_i > 1$ for all $i > 1$ (see Exercise 1.6.5).

Exercises

3.2.15 Show that S_7 acting on the set of 3-subsets of $\{1, 2, \ldots, 7\}$ has degree 35 and rank 4 with subdegrees 1,4,12,18.

3.2.16 Using the notation above, show that if either $n_i \geq n/2$, or $n_i \geq n/4$ and the corresponding orbital Δ_i is not self-paired, then any two vertices in Graph(Δ_i) can be joined by a nondirected path of length ≤ 2.

Lemma 3.2B. *Let G be a finite primitive permutation subgroup of Sym(Ω) of degree n and rank $r > 2$ with subdegrees $n_1 = 1 \leq n_2 \leq \ldots \leq n_r$. Assume that G is not regular. Then*

(i) *$n_{i+1} \leq n_i(n_2 - 1)$ for all $i \geq 2$;*

(ii) *the largest subdegree n_r has a nontrivial factor in common with n_i for each $i = 2, \ldots r - 1$;*

(iii) *if k of the subdegrees $n_2, \ldots, n_{r-1}$ are pairwise relatively prime then $r \geq 2^k$.*

PROOF. (i) When G is a finite we can refine the arguments of Theorem 3.2B (iii) as follows. Fix $\alpha \in \Omega$, and order the orbitals $\Delta_1, \ldots, \Delta_r$ such that $|\Delta_i(\alpha)| = n_i$ for each i. To simplify notation, set $\Delta := \Delta_2$ and let Δ^* be its paired orbital. The set $\Delta \circ \Delta^*$ is G-invariant and consists of all pairs (α, β) such that $(\alpha, \gamma), (\beta, \gamma) \in \Delta$ for some γ. Moreover, $\Delta \circ \Delta^*$ contains a nondiagonal orbital because $n_2 > 1$.

Now consider paths in the colour graph of G which start at α and have the form: $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_k$ with each edge (α_i, α_{i+1}) in either Δ or Δ^* depending on whether i is even or odd. We shall call such a path an "alternating path" of length k. Since $\Delta \circ \Delta^*$ contains a nondiagonal orbit, Theorem 3.2B (ii) shows that for each $\beta \in \Omega$ there is an alternating path from α to β.

Suppose that $2 \le i < r$; we want to show that $n_{i+1} \le n_i(n_2 - 1)$. Let k be the shortest length of a minimal alternating path from α to some vertex β for which $(\alpha, \beta) \in \Delta_j$ and $j > i$. Fix such a path, $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_k = \beta$, and note that $k \ge 2$ because $j \ne i$. By the choice of k, $(\alpha, \alpha_{k-1}) \in \Delta_t$ for some $t \le i$. Now suppose that k is odd (the case where k is even is analogous with Δ replaced by Δ^*). In the colour graph, there are n_2 edges out of α_{k-1} from Δ, and one of these goes to α_{k-2}. Hence there are at most $n_2 - 1$ points $\gamma \in \Delta_j(\alpha)$ such that $(\alpha_{k-1}, \gamma) \in \Delta$. On the other hand, $\Delta_j(\alpha)$ is a G_α-orbit containing β, and there is an alternating path of length k from α to each point $\beta^x \in \Delta_j(\alpha)$ with $x \in G_\alpha$ given by: $\alpha = \alpha^x, \alpha_1^x, \ldots, \alpha_{k-1}^x, \beta^x$. Now $\alpha_{k-1}^x \in \Delta_t(\alpha)$ for all $x \in G_\alpha$, and so can only take $|\Delta_t(\alpha)| = n_t$ values. Hence β^x can take at most $n_t(n_2 - 1)$ values. Thus $n_{i+1} \le n_j \le n_t(n_2 - 1) \le n_i(n_2 - 1)$ as required. The proofs of parts (ii) and (iii) are left to Exercises 3.2.18, 3.2.19 and 3.2.20. The first two of these exercises are actually quite general and apply to infinite groups as well. □

Exercises

3.2.17 Calculate the rank and subdegrees for the following groups:
  (i) The wreath product $S_m \; wr \; S_2$ with the product action of degree m^2;
  (ii) S_m acting on the set of 2-sets of degree $m(m-1)/2$;
  (iii) $S_m \; wr \; S_m$ acting imprimitively of degree m^2;
  (iv) The subgroup of the group in (iii) given by $D_{2m} \; wr \; S_m$ where D_{2m} is a dihedral group of order $2m$ acting transitively.

3.2.18 If the group G acts transitively on two finite sets Γ and Δ whose sizes are relatively prime, show that the natural action of G on $\Gamma \times \Delta$ is also transitive.

3.2.19 Let G be a transitive group on a set Ω and α a point in Ω. Let Δ and Γ be orbitals of G for which $m := |\Delta(\alpha)|$ and $n := |\Gamma(\alpha)|$ are finite and relatively prime with $m \le n$. Show that $\Delta \circ \Gamma$ is an orbital for G, that $k := |\Delta \circ \Gamma(\alpha)|$ is also finite and divides mn, and that $k \ge n$. If $m > 1$ and G is primitive, show that $k > n$.

3.2.20 Use the previous exercise to show that, for a finite, nonregular, primitive permutation group, the largest subdegree has a nontrivial factor in common with each of the other nontrivial subdegrees. In particular, if the group has k relatively prime nontrivial subdegrees, then its rank is at least 2^k.

3.2.21 Let p be an odd prime. Show that there is no primitive group of degree $p + 1$ and rank 3.

3.2.22 Show that a primitive group of degree 6, 8 or 12 must be 2-transitive.

The previous results are basically combinatorial. The following result gives a group theoretic restriction on the structure of a point stabilizer of a

primitive group acting on a suborbit. Recall that S is a *section* of a group G if for some subgroups H and K of G we have $K \lhd H$ and $H/K \cong S$.

Theorem 3.2C. *Suppose that G is a finite primitive subgroup of $Sym(\Omega)$. Let $\alpha \in \Omega$ and let Γ be a nontrivial orbit of G_α. Then every simple section of G_α is isomorphic to a section of the group G_α^Γ which G_α induces on Γ. In particular, each composition factor of G_α is isomorphic to a section of G_α^Γ.*

PROOF. We first show that if $1 < H \leq G_\alpha$ and $\beta \in \Gamma$ then, for some $x \in G, x^{-1}Hx$ fixes α but does not fix β. Indeed, put $\Delta := \mathrm{fix}(H)$ and note that $\Delta \neq \Omega$ because $H \neq 1$. If $\beta \notin \Delta$ we can take $x = 1$, so assume $\beta \in \Delta$. Now because G is primitive, Δ is not a block for G and so for some $x \in G$ we have $\alpha \in \Delta^x = \mathrm{fix}(x^{-1}Hx)$ and $\beta \notin \Delta^x$ (see Exercise 1.5.5).

Now suppose that S is a simple group which is isomorphic to a section of G_α. Choose $H \leq G_\alpha$ which is minimal with respect to the condition that $S \cong H/K$ for some $K \lhd H$. Since S is simple, K is a maximal normal subgroup of H, and so if $N \lhd H$ and N is not contained in K, then $S \cong H/K = NK/K \cong N/(N \cap K)$. Thus, by the choice of H we conclude that K contains all proper normal subgroups of H, and so every nontrivial homomorphic image of H contains a section isomorphic to S. On the other hand, from what we showed at the beginning of this proof, there exists $x \in G$ such that $x^{-1}Hx \leq G_\alpha$ and $(x^{-1}Hx)^\Gamma \neq 1$. The restriction G_α^Γ of G_α to Γ contains $(x^{-1}Hx)^\Gamma$ and so has a section isomorphic to $(x^{-1}Hx)/(x^{-1}Kx) \cong S$, and the theorem is proved. □

Corollary 3.2A. *If G is a finite, nonregular, primitive group and $\Gamma \neq \{\alpha\}$ is an orbit of a point stabilizer G_α, then:*
(i) *each prime dividing $|G_\alpha|$ also divides $|G_\alpha^\Gamma|$;*
(ii) *G_α is solvable whenever G_α^Γ is solvable.*

For further results along these lines see Sect. 4.4. This section concludes with an application of Corollary 3.2A on the support of a Sylow p-subgroup. It is an interesting example of how reduction to the primitive case is used.

Theorem 3.2D. *Let $G \leq Sym(\Omega)$ be a transitive group of degree n, and let P be a Sylow p-subgroup of G. If $P \neq 1$ then $|\mathrm{fix}(P)| < n/2$.*

PROOF. The result is true for $n \leq 3$, so we can proceed by induction. Assume $n > 3$ and $P \neq 1$. We consider two cases.

First, suppose that G is primitive. We may assume that P fixes at least one point, say α, since otherwise the assertion is trivially true. Let $\Omega_1 := \{\alpha\}, \Omega_2, \ldots, \Omega_r$ be the orbits of G_α of lengths $n_1 = 1, n_2, \ldots, n_r$, respectively. Since $1 \neq P \leq G_\alpha$, Corollary 3.2A (i) shows that P acts nontrivially on each of the orbits Ω_i $(i > 1)$, and hence by induction

$|\text{fix}(P) \cap \Omega_i| \leq (n_i - 1)/2$ for each $i > 1$. Hence

$$|\text{fix}(P)| \leq 1 + \sum_{i=2}^{r} \frac{n_i - 1}{2} = \frac{(n - r + 2)}{2} \leq \frac{n}{2}.$$

We claim that equality cannot hold in this inequality. Indeed, $p \nmid n = |G : G_\alpha|$ because P is a Sylow p-subgroup of G and $P \leq G_\alpha$. However, p does divide $|\text{supp}(P)| = n - |\text{fix}(P)|$ because each orbit of P has p-power length, and so $|\text{fix}(P)| \neq n/2$. Thus $|\text{fix}(P)| < n/2$ when G is primitive.

Now suppose that G is imprimitive, and let $\Sigma := \{\Delta_1, \ldots, \Delta_m\}$ be a system of m blocks each of size d, say, where $n = md$ and $1 < d < n$. Let K be the kernel of the action of G on Σ. Since Δ_i is a block, $P \leq G_{\{\Delta_i\}}$ whenever $\Delta_i \cap \text{fix}(P) \neq \emptyset$, and therefore P must fix (setwise) at least $|\text{fix}(P)|/d$ of the blocks in Σ. If P is not contained in K, then P acts nontrivially on Σ and induction shows that $|\text{fix}(P)|/d < m/2$, and hence $|\text{fix}(P)| < n/2$ as required. On the other hand, suppose that $P \leq K$. Since the induced groups K^{Δ_i} $(i = 1, \ldots, m)$ are isomorphic, each must have order divisible by p. If $\Delta_i \subseteq \text{fix}(P)$, then $\Delta_i \subseteq \text{fix}(u^{-1}Pu)$ for all $u \in K$, and so all the Sylow p-subgroups of K would act trivially on Δ_i which is impossible. Thus P acts nontrivially on each of the m blocks Δ_i, and so induction shows that $|\text{fix}(P)| < md/2 = n/2$ as required. This proves the theorem. □

Exercises

3.2.23 Let G be the image of the (primitive) action of S_8 on the set of 3-sets of $\{1, 2, \ldots, 8\}$. Using the fact that A_5 is simple, show that A_5 is a composition factor for a point stabilizer G_α of G, but not a composition factor of G_α^Γ for some nontrivial orbit of Γ of G_α. (This shows that we cannot replace "section" by "composition factor" in Theorem 3.2C.)

3.2.24 If G is a finite primitive group with subdegrees $1 = n_1 < n_2 \leq \ldots \leq n_r$, show that $p \leq n_2$ for each prime p dividing n_i $(i = 3, \ldots, r)$.

3.2.25 Let G be a finite primitive group with a subdegree equal to a prime p. Show that p divides $|G_\alpha|$ but p^2 does not. [*Hint:* choose an orbital Δ of G such that $|\Delta(\alpha)| = p$, and let $\beta \in \Delta(\alpha)$. Use induction to show that each of the sets $\Delta(\alpha), \Delta \circ \Delta^*(\alpha), \Delta \circ \Delta^* \circ \Delta(\alpha), \ldots$ is fixed pointwise by any p-subgroup of $G_{\alpha\beta}$.]

3.2.26 Let G be a primitive, but not 2-transitive, group of degree 10.
   (i) Show that G has rank 3 and subdegrees 1, 3 and 6.
   (ii) If Δ is the orbital corresponding to the subdegree 3, show that Graph(Δ) is isomorphic to the Petersen graph (Exercise 2.3.4).
   (iii) Conclude that G is permutation isomorphic to A_5 or S_5 acting on 2-sets of $\{1, 2, 3, 4, 5\}$.

3.2.27 Suppose that G acts as a transitive group with point stabilizer H. Show that G has rank r in this action if and only if there are elements

$y_i \in G$ for $i = 1, \ldots, r$ such that G is the disjoint union of the double cosets

$$G = \bigcup_{i=1}^{r} Hy_iH.$$

In particular, G is 2-transitive if and only if $G = H \cup HyH$ for some $y \in G$.

3.2.28 Let F be a finite field with an odd number of elements. Let $\mathcal{G}$ be the digraph with vertex set F where (α, β) is an edge $\iff \alpha - \beta$ is a nonzero square in F. Show that $\mathrm{Aut}(\mathcal{G})$ acts transitively on F, and find its rank and order.

3.2.29 Show that every primitive group of degree 20 is 2-transitive.

3.3 Minimal Degree and Bases

A basis is a very important and useful tool in studying vector spaces and linear transformations. In particular, every linear transformation is completely determined by how it acts on a basis. An analogous idea is useful in the study of permutation groups. Let G be a group acting on the set Ω. A subset Σ of Ω is called a *base* for G if $G_{(\Sigma)} = 1$; in other words the identity is the only element of G which fixes every element in Σ.

Exercises

3.3.1 Suppose G is a group acting on Ω and $\Sigma \subseteq \Omega$. Show that the following are equivalent:
(i) Σ is a base for G;
(ii) Σ^x is a base for G for all $x \in G$;
(iii) for all $x, y \in G$, $(\alpha^x = \alpha^y$ for all $\alpha \in \Sigma)$ implies $(x = y)$;
(iv) $\Sigma \cap \mathrm{supp}(x) \neq \emptyset$ for all $x \neq 1$ in G.

3.3.2 If G is a finite permutation group of degree n and a smallest base for G has size b, show that $2^b \leq |G| \leq n(n-1)\ldots(n-b+1) \leq n^b$.

If a group G acting on a set Ω has nontrivial elements with finite support, we define the *minimal degree* of G to be the minimum of $|\mathrm{supp}(x)|$ for all $x \in G, x \neq 1$. Exercise 3.3.1 suggests that in cases where the minimal degree is small, the bases of G must be large. An extreme case is S_n which has minimal degree 2 and whose smallest base has size $n - 1$.

Exercises

3.3.3 Consider the affine group $AGL_d(F)$ acting on F^d where $F = \mathbb{F}_q$ is the finite field with q elements (see Sect. 2.8). The degree of this action is q^d. Show that the minimal degree is $q^{d-1}(q-1)$, and the size of the smallest base is $d + 1$.

3.3.4 Find the minimal degrees and minimum base sizes for the following groups:
 (i) A_n;
 (ii) the wreath product $S_d \ wr \ S_r$ with the imprimitive action of degree dr;
 (iii) the wreath product $S_d \ wr \ S_r$ with the product action of degree d^r;
 (iv) the 3-transitive action of $PGL_2(F)$ on $PG_1(F)$, the set of "lines" of F^2, where $F = \mathbb{F}_q$ is the finite field with q elements (see Sect. 2.8).

3.3.5 Let $m \geq 5$ and consider the action of S_m on the set of 2-sets of $\{1, 2, \ldots, m\}$. This action is primitive of degree $n := m(m-1)/2$. Show that the minimal degree is $2m - 4$ and that there is a base of size $\lfloor 2m/3 \rfloor$. (The latter is less than $\sqrt{n}$ if $m \geq 10$.)

3.3.6 Suppose that G is a (possibly infinite) primitive group. If G contains an element x with $|\mathrm{supp}(x)| = m$ and x has s nontrivial disjoint cycles, show that G has rank at most $m - s + 1$. In particular, if G has minimal degree m then G has rank at most m. Give examples to show that this is not necessarily true for transitive groups. [*Hint:* Choose $\alpha \in \mathrm{supp}(x)$, and note that $G = \langle x, G_\alpha \rangle$ because G is primitive.]

Exercises 3.3.4 (i) and (ii) gives examples of transitive groups of arbitrarily large degree with small minimal degree. Notice however that in none of these cases are the groups properly primitive (that is, primitive and distinct from the alternating and symmetric groups of same degree). This is no accident, as Theorem 3.3C shows. In fact one of the main results of Chap. 5 will give a lower bound on the minimal degree of a proper primitive group in terms of the degree of the group. As a first modest step we examine groups with minimal degree 2 or 3. Recall that the finitary symmetric group $FSym(\Omega)$ consists of all permutations of Ω with finite support (see Exercise 1.6.6). In the arguments below we shall be frequently calculating expressions of the type $y^{-1}xy$ and $x^{-1}y^{-1}xy$ (recall Exercise 1.2.6).

Theorem 3.3A. *Let G be a primitive subgroup of $Sym(\Omega)$.*
 (i) *If G contains a 3-cycle, then $G \geq Alt(\Omega)$.*
 (ii) *If G contains a 2-cycle, then $G \geq FSym(\Omega)$. In particular, if Ω is finite, then $G = Sym(\Omega)$.*

PROOF. (i) If $\Delta \subseteq \Omega$, then we shall identify $Alt(\Delta)$ with the subgroup of $Alt(\Omega)$ consisting of all elements which fix $\Omega \setminus \Delta$ pointwise. Let Δ be a maximal subset of Ω with the property that $G \geq Alt(\Delta)$ (the proof that such a subset exists when Ω is infinite requires Zorn's Lemma or an equivalent transfinite argument). By hypothesis $|\Delta| \geq 3$, and we want to show that $\Delta = \Omega$. Suppose that $\Delta \neq \Omega$.

Since G is primitive, Δ is not a block for G, and so there exists $x \in G$ such that $\Delta \cap \Delta^x \neq \emptyset$ or Δ. First suppose that $\Delta \cap \Delta^x$ contains only one

element, say α. Since $x^{-1}Alt(\Delta)x = Alt(\Delta^x)$, and $G \geq Alt(\Delta)$, therefore there are 3-cycles of the form $y := (\alpha\beta\gamma)$ and $z := (\alpha\delta\eta)$ in G with $\beta, \gamma \in \Delta$ and $\delta, \eta \in \Delta^x$. Then G contains $z^{-1}y^{-1}zy = (\alpha\beta\delta)$ with exactly two points in Δ. On the other hand, if $\Delta \cap \Delta^x$ contains at least two points, say α and β, then choose $\delta \in \Delta^x \setminus \Delta$. Since α, β and δ all lie in Δ^x, again G contains a 3-cycle $(\alpha\beta\delta)$ with exactly two points in Δ.

Thus let $w := (\alpha\beta\delta) \in G$ with $\alpha, \beta \in \Delta$ and $\delta \notin \Delta$, and put $\Gamma := \Delta \cup \{\delta\}$. We claim that $G \geq Alt(\Gamma)$. Since $G \geq Alt(\Delta)$, it is enough to show that $u \in G$ for all $u \in Alt(\Gamma)$ with $\delta^u \neq \delta$. Since $\epsilon := \delta^u \in \Delta$, there exists $v \in Alt(\Delta)$ such that $\epsilon^v = \beta$, and then $uv(\alpha\beta\delta) \in Alt(\Gamma)$ and fixes δ. This implies that $uv(\alpha\beta\delta)$ and $v(\alpha\beta\delta)$ both lie in G and so $u \in G$. Hence $G \geq Alt(\Gamma)$ contrary to the maximality of Δ. This shows that $\Delta = \Omega$ as required.

(ii) Clearly we may assume that $|\Omega| \geq 3$. Suppose G contains the 2-cycle $(\alpha\beta)$. Then $\{\alpha, \beta\}$ is not a block for G, and so there exists $x \in G$ such that $\{\alpha, \beta\} \cap \{\alpha, \beta\}^x$ has size 1. Relabelling if necessary we can assume that $\{\alpha, \beta\}^x = \{\alpha, \gamma\}$ with $\gamma \neq \beta$. Now $(\alpha\beta)x^{-1}(\alpha\beta)x = (\alpha\beta)(\alpha\gamma) = (\alpha\beta\gamma)$ lies in G, so $G \geq Alt(\Omega)$ by (i). But $(\alpha\beta)$ is an odd permutation and so $G \geq \langle(\alpha\beta), Alt(\Omega)\rangle = FSym(\Omega)$. □

As an immediate application of this theorem we show that $Alt(\Omega)$ is a (nonabelian) simple group when $|\Omega| \geq 5$. We remark that $Alt(\Omega)$ is a simple (cyclic) group when $|\Omega| = 2$ or 3, and that $Alt(\Omega)$ is not simple when $|\Omega| = 4$.

Corollary 3.3A. *If $|\Omega| \geq 5$, then $Alt(\Omega)$ is simple.*

PROOF. Put $A := Alt(\Omega)$ with $|\Omega| \geq 5$. Suppose we have $N \lhd A$ and $N \neq 1$; then N is transitive by Theorem 1.6A and the primitivity of $Alt(\Omega)$. Since $N \leq A$, the minimal degree m of N is at least 3. Our first step is to prove that $m = 3$. Every element of finite support has finite order, and so we can choose an element $u \in N$ of prime order, say p, and all of the nontrivial cycles of u have length p. We observe that if $x \in A$, then the commutator $y := [u^{-1}x^{-1}u, x] = u^{-1}(xux^{-1})u^{-1}(x^{-1}ux) \in N$. In particular, if $|\text{supp}(u^{-1}x^{-1}u) \cap \text{supp}(x)| = 1$, then N contains a 3-cycle by Exercise 1.6.7. Consider three special cases:

(i) If $p > 3$, then u has a cycle $(\alpha\beta\gamma\delta\epsilon\ldots)$ of length at least 5. Take $x = (\alpha\beta\delta)$, and then $y = (\beta\delta\gamma) \in N$.

(ii) If $p = 3$, and u is not a 3-cycle, then u has at least two 3-cycles $(\alpha\beta\gamma)(\delta\epsilon\theta)\ldots$. Take $x = (\alpha\beta\delta)$, and then $y = (\beta\delta\gamma) \in N$.

(iii) If $p = 2$, then u has at least two 2-cycles $(\alpha\beta)(\gamma\delta)\ldots$. Take $x = (\alpha\beta\gamma)$, and then $y = (\alpha\beta)(\gamma\delta) \in N$.

It follows from (i) and (ii) that $m = 3$ if $p > 2$. In the case $p = 2$, (iii) shows that u can be chosen in the form $(\alpha\beta)(\gamma\delta)(\epsilon)\ldots$; taking $x = (\alpha\gamma\epsilon)$

in this case gives $y = (\alpha\beta\epsilon) \in N$. Thus in all cases $m = 3$ as asserted, and N contains a 3-cycle z.

Finally, since A is 3-transitive, $x^{-1}zx$ runs over the set of all 3-cycles of A as x runs over A; hence N contains all 3-cycles. This implies that N has no nontrivial blocks, and so N is primitive (see Exercise 1.5.5). Thus $N = A$ by the theorem. This shows that A has no proper nontrivial normal subgroups, and so A is simple. □

As another application of the theorem we shall prove a classical result on the size of a base for a primitive group due to Bochert (1889). The bound is crude but frequently useful. See Chapter 5 for better bounds.

Theorem 3.3B. *Let $G \leq Sym(\Omega)$ be a proper primitive group of finite degree n. Then G has a base of size at most $n/2$, and so $|G| \leq n(n-1)\cdots(n - \lfloor n/2 \rfloor + 1)$.*

PROOF. It is enough to prove the first statement; the bound on the order of G then follows from Exercise 3.3.2.

Let G be a primitive subgroup of $Sym(\Omega)$, and let Σ be a base for G of minimal size. Suppose that $|\Sigma| > n/2$; we shall show that $G \geq Alt(\Omega)$. Indeed, $|\Sigma| > n/2$ implies that $\Delta := \Omega \setminus \Sigma$ is not a base by the minimality of Σ. Thus there exists $x \neq 1$ in G with support disjoint from Δ (see Exercise 3.3.1), and so $\mathrm{supp}(x) \subseteq \Sigma$. Choose $\alpha \in \mathrm{supp}(x)$. Since $\Sigma \setminus \{\alpha\}$ is not a base for G by the choice of Σ, there exists $y \neq 1$ in G such that

$$\mathrm{supp}(y) \subseteq \Omega \setminus (\Sigma \setminus \{\alpha\}) = \Delta \cup \{\alpha\}.$$

Since Σ is a base, $\mathrm{supp}(y) \cap \Sigma \neq \emptyset$, and so $\alpha \in \mathrm{supp}(y)$. Therefore $\mathrm{supp}(x) \cap \mathrm{supp}(y) = \{\alpha\}$, and so G contains a 3-cycle by Exercise 1.6.7. Hence $G \geq Alt(\Omega)$ by Theorem 3.3A. Thus we conclude that if G is a proper primitive group then $|\Sigma| \leq n/2$ as asserted. □

Table 3.2 compares the maximal order $\mathrm{M}(n)$ of a proper primitive group of degree n with the Bochert bound $\mathrm{B}(n)$ given by the last theorem.

Our next immediate objective is to prove a relationship between degree, minimum base size and minimal degree which holds for any transitive

TABLE 3.2. The Orders of Primitive Groups and Bochert's Bound

$n =$	5	6	7	8	9	10	11	12
$\mathrm{M}(n) =$	20	120	168	1344	1512	1440	7920	95040
$\mathrm{B}(n) =$	20	120	210	1680	3024	30240	55440	665280

group. If the group involved is finite, then there is a simple counting argument to prove this result (see Exercise 3.3.7), but the general case needs a different approach.

Exercise

3.3.7 Let G be transitive subgroup of $Sym(\Omega)$ where Ω is finite, and suppose that the minimal base size of G is b and the minimal degree is m. Show that $|\Omega| \leq bm$. [*Hint:* Let Σ be a base of minimal size and let Δ be the support of an element of minimal degree. Show that $|\Sigma^x \cap \Delta| \geq 1$ for all $x \in G$ and that, for each $\alpha \in \Omega$, there are exactly $|\Sigma| |G| /n$ values of $x \in G$ such that $\alpha \in \Sigma^x$. Hence $|\Delta| |\Sigma| |G| /n = \sum_{x \in G} |\Sigma^x \cap \Delta| \geq |G|$.]

To deal with the general case we begin with a result due to B.H. Neumann (1954).

Lemma 3.3A. *Let G be an arbitrary group and let H_i $(i = 1, \dots, m)$ be subgroups of G. If G is a union of left cosets*

$$G = \bigcup_{i=1}^{m} H_i x_i \tag{3.1}$$

for some elements $x_i \in G$, then $|G : H_i| \leq m$ for at least one i.

PROOF. Without loss in generality we may suppose that the union in (3.1) is "irredundant", that is, no proper subset of the set of cosets $H_i x_i$ $(i = 1, \dots, m)$ has its union equal to G. We shall first show that under this assumption all H_i have finite index in G.

We proceed by induction on the number of distinct H_i. If all H_i are equal then the assertion is clearly true, so suppose that at least two are different, and let one of these subgroups be denoted by K. Since we are assuming the union in (3.1) is irredundant, some coset Ku of K in G does not appear in (3.1). Then

$$Ku \subseteq \bigcup \{H_i x_i \mid H_i \neq K\}$$

and using this we can replace each term $H_j x_j$ in (3.1) which has $H_j = K$ by a union of a finite number of cosets in the H_i which are different from K. The inductive hypothesis then shows that all H_i distinct from K have finite index in G. Since K was chosen arbitrarily from among the H_i, this shows that $|G : H_i|$ is finite for all i.

Since all H_i have finite index in G, there exists $N \triangleleft G$ of finite index in G with $N \leq H_i$ for all i (see Exercise 3.3.8 below). If we write $\overline{x}_i := Nx_i$, then (3.1) shows that

$$G/N = \bigcup_{i=1}^{m} (H_i/N)\overline{x}_i$$

and so

$$|G : N| \leq \sum_{i=1}^{m} |H_i : N| .$$

Hence for the value of j for which $\left|H_j : N\right|$ is largest we have $\left|G : H_j\right| = \left|G/N : H_j/N\right| \leq m$ as required. □

Exercises

3.3.8 Let H_i ($i = 1, \ldots, m$) be subgroups of finite index in a group G. Show that G has a normal subgroup of finite index which is contained in every H_i. [*Hint:* Consider the action of G by right multiplication on the set of all right cosets of the H_i.]

3.3.9 Under the hypothesis of Lemma 3.3.A and assuming that the union in (3.1) is irredundant, show that $|G : \cap H_i| \leq m!$.

Exercise 3.3.1 shows that a base Σ for a group G has a nonempty intersection with the support of every nontrivial element. The following theorem is concerned with this sort of situation in a general setting.

Theorem 3.3C. *Let $G \leq Sym(\Omega)$ and suppose that Γ and Δ are finite subsets of Ω of sizes m and n, respectively. If $\Gamma^x \cap \Delta \neq \emptyset$ for all $x \in G$, then at least one point of Γ lies in an orbit of G of length $\leq mn$.*

Proof. For each $\gamma \in \Gamma$ and each $\delta \in \Delta \cap \gamma^G$ we choose $x_{\gamma\delta} \in G$ mapping γ to δ. Then the hypothesis shows that every $x \in G$ lies in at least one of the cosets $G_\gamma x_{\gamma\delta}$. Since there are at most mn of these cosets, Lemma 3.3A now shows that for some $\gamma \in \Gamma$ we have $\left|G : G_\gamma\right| \leq mn$, and so the orbit γ^G has length $\leq mn$ as required. □

Exercises

3.3.10 For any positive integers m, n find a transitive group G of degree mn on a set Ω and subsets Δ and Γ of sizes m and n, respectively, such that $\Gamma^x \cap \Delta \neq \emptyset$ for all $x \in G$. [*Hint:* Choose Γ and Δ as blocks for G.]

3.3.11 Show that the following natural analogue of Theorem 3.3C is false: "If $G \leq Sym(\Omega)$ and Δ, Γ are countably infinite subsets of Ω such that $\Gamma^x \cap \Delta \neq \emptyset$ for all $x \in G$, then G has an orbit which is of at most countable length." [*Hint:* Let $G = Alt(\Omega)$ where Ω is uncountable.]

3.3.12 Give an example of a group G which is a union of a countable number of proper subgroups but which does not have any proper subgroup of countable index.

Corollary 3.3B. *Let G be a transitive subgroup of $Sym(\Omega)$. If G has finite minimal degree m and a finite base of size b, then Ω is finite and $|\Omega| \leq bm$.*

PROOF. Let $\Delta := \text{supp}(z)$ for some $z \in G$ with $|\Delta| = m$, and let Σ be a base of size b. Then $\Sigma^x \cap \Delta \neq \emptyset$ for all $x \in G$ by Exercise 3.3.1. The result now follows from Theorem 3.3C and the transitivity of G. □

Exercise

3.3.13 Give an example to show that the conclusion of Corollary 3.3B may be false if G is not assumed to be transitive.

We are now in a position to prove a theorem due to Jordan (1871) on the minimal degree of proper primitive permutation groups. The case where the minimal degree is 2 or 3 has been dealt with in Theorem 3.3A.

Theorem 3.3D. *For each integer $m \geq 4$ there exists a constant β_m such that if G is a proper primitive subgroup of $Sym(\Omega)$ and G contains an element z with $|\text{supp}(z)| = m$, then $|\Omega| \leq \beta_m$; and if G is 2-transitive, then $|\Omega| \leq 1 + (m-1)^2$. In particular, if Ω is infinite, then every primitive subgroup of $Sym(\Omega)$ containing a nontrivial element of $FSym(\Omega)$ must contain $Alt(\Omega)$.*

PROOF. Choose $\alpha \in \text{supp}(z)$ and put $\Delta := \text{supp}(z) \setminus \{\alpha\}$. We first note that $\Delta^x \cap \Delta \neq \emptyset$ for all $x \in G_\alpha$. Indeed, otherwise $\text{supp}(x^{-1}zx)$ and $\text{supp}(z)$ have exactly one point in common and G contains a 3-cycle (see Exercise 1.6.7); this is impossible by Theorem 3.3A because G does not contain $Alt(\Omega)$. Theorem 3.3C now shows that G_α has an orbit $\Gamma \neq \{\alpha\}$ of length $\ell \leq (m-1)^2$. On the other hand the rank r of G is at most m by Exercise 3.3.6. Thus Theorem 3.2B (iii) shows that

$$|\Omega| \leq 1 + \ell + \ell^2 + \ldots + \ell^{r-1} < \ell^r \leq (m-1)^{2m}.$$

This proves the first statement with $\beta_m := (m-1)^{2m}$.

In the case where G is 2-transitive, then $r = 2$, and so the estimate above gives $|\Omega| \leq 1 + (m-1)^2$ as asserted. □

The proof above shows that we can take $\beta_m = (m-1)^{2m}$, but this is a very crude estimate. Similarly the estimate for the 2-transitive case is quite crude. Much better bounds are obtained later in Chap. 5.

The following example due to Jordan (1875) shows how it is possible to strengthen these estimates in the case where $m = 4$.

EXAMPLE 3.3.1. We shall show that if $G \leq S_n$ is a primitive group with minimal degree 4, then $n \leq 8$. We shall leave the cases $n = 9, 10$ and 11 as an exercise (Exercise 3.3.14), and obtain a contradiction under the assumption that $n \geq 12$. Since the square of a 4-cycle is of type 2^2 (that is, a product of two 2-cycles), the group G contains an element of type 2^2, and so we may suppose that $u := (12)(34) \in G$. Since 4 is the minimal degree, G is proper primitive and Exercise 3.3.6 shows that G has rank 2

or 3. Theorem 3.3D shows that G cannot be 2-transitive because $n > 10$, and so G has rank 3. Let the orbits of G_1 be $\{1\}, \Gamma$ and Δ, of lengths $1, c$ and d, respectively. Again the condition on n and Lemma 3.2B (i) show that c and d are both at least 4.

Since $G = \langle G_1, u\rangle$ by the primitivity of G, neither Γ nor Δ can contain a nontrivial orbit of u. Hence, relabeling the points and orbits if necessary, we may assume $2, 3 \in \Gamma$ and $4 \in \Delta$. Put $h := |G_1|$ and define

$$B_{\alpha\beta} := \{x \in G_1 \mid \alpha^x = \beta\} \quad \text{for } \alpha, \beta \in \{2, 3, 4\}.$$

For each pair (α, β), either $B_{\alpha\beta}$ is empty or it is a coset of the point stabilizer $G_{1\alpha}$ in G_1. Hence the orbit-stabilizer theorem shows that $|B_{\alpha\beta}| = h/c$ if $\alpha, \beta \in \{2, 3\}$, $|B_{44}| = h/d$, and the other $B_{\alpha\beta}$ are empty.

We claim that the union of the $B_{\alpha\beta}$ is equal to G_1. Indeed, suppose that y is an element of G_1 not lying in any $B_{\alpha\beta}$. Then $\mathrm{supp}(u) \cap \mathrm{supp}(y^{-1}uy) = \{1\}$, and so G contains a 3-cycle by Exercise 1.6.7, contradicting the assumption that G has minimal degree 4. In particular, since $c \geq 4, d \geq 4$ and $c + d \geq 11$, the inequality

$$h = \left|\cup B_{\alpha\beta}\right| \leq \sum \left|B_{\alpha\beta}\right| = \frac{4h}{c} + \frac{h}{d}$$

shows that $c = 4$.

Finally, we show that the case $c = 4$ is impossible. In this case $G_1^{\Gamma} \leq Sym(\Gamma)$ is transitive of degree 4, and so is either $Sym(\Gamma)$, $Alt(\Gamma)$, a dihedral group of order 8, or an elementary abelian 2-group of order 4. In the respective cases, we can verify that $|B_{22} \cap B_{33}| = |G_{123}| = h/24, h/12, h/8$ or $h/4$, and that $|B_{23} \cap B_{32}| = 2h/24, h/12, 2h/8$ or $h/4$. Thus, since $|B_{22} \cap B_{44}| \geq 1$, we have

$$\begin{aligned} h = \left|\cup B_{\alpha\beta}\right| &\leq \sum \left|B_{\alpha\beta}\right| - |B_{22} \cap B_{33}| - |B_{23} \cap B_{32}| - 1 \\ &\leq \frac{4h}{c} + \frac{h}{d} - \frac{3h}{24} - 1. \end{aligned}$$

Since $c = 4$, this implies that $d < 8$. Since $c + d \geq 11$, this means that $d = 7$, but then Lemma 3.2B (ii) shows that this is impossible because 4 and 7 are relatively prime.

Exercises

3.3.14 Suppose that $G \leq S_n$ is a primitive group of rank 3 with a subdegree 3. If G contains an element of type 2^2, show that $n = 7$ or 10. Is the group uniquely determined in each case? (See also Exercise 3.2.26.)

3.3.15 Let G be a primitive group of degree n and of minimal degree 4. Show that n is not equal to 9, 10 or 11. Find all examples of such groups when $n \leq 8$.

We conclude this section with one further theorem of Jordan which is often useful in discussing finite primitive groups. It is a special case of a general class of results which will be discussed later in Sect. 7.4.

Theorem 3.3E. *Let $G \leq Sym(\Omega)$ be a primitive group which contains a cycle x of prime length p. Then either $G \geq Alt(\Omega)$ or $|\Omega| \leq p + 2$.*

PROOF. Theorems 3.3D and 3.3A show that the result holds if either Ω is infinite or $p = 2$ or 3. So suppose that Ω is finite of size n and $p \geq 5$, and assume that $n \geq p + 3$; we must show that $G \geq Alt(\Omega)$. As a first step we shall show that G is 2-transitive and that, for each $\alpha \in \Omega$, G_α acts primitively on $\Omega \setminus \{\alpha\}$.

Consider the set $\mathcal{S}$ consisting of all $\Gamma \subseteq \Omega$ such that $\Gamma \neq \Omega$ and $G_{(\Omega \setminus \Gamma)}$ acts primitively on Γ. Then $\mathcal{S} \neq \emptyset$ because $\mathrm{supp}(x) \in \mathcal{S}$, and Exercise 3.3.16 shows that: if $\Delta, \Gamma \in \mathcal{S}$ with $\Delta \cap \Gamma \neq \emptyset$ and $\Delta \cup \Gamma \neq \Omega$, then $\Delta \cup \Gamma \in \mathcal{S}$. Let Δ be a maximal element of $\mathcal{S}$ containing $\mathrm{supp}(x)$; we claim that $|\Delta| = n - 1$. Indeed, since G is primitive, then there exists $y \in G$ such that $\Delta^y \cap \Delta \neq \emptyset$ or Δ. Clearly, $\Delta^y \in \mathcal{S}$, so the observation above shows that $\Delta^y \cup \Delta = \Omega$ by the maximality of Δ. This implies that $n < 2|\Delta|$. Now, suppose that $\delta \in \Omega \setminus \Delta$. Then for all $z \in G_\delta$, $\Delta \cap \Delta^z \neq \emptyset$ because $|\Delta| > n/2$, and $\delta \notin \Delta \cup \Delta^z$, so the observation above shows that $\Delta \cup \Delta^z \in \mathcal{S}$. Thus the maximality of Δ shows that $\Delta = \Delta^z$ for all $z \in G_\delta$. Since G is primitive, G_δ is a maximal subgroup of G, and so $G_\delta = G_{\{\Delta\}}$. Since this is true for all points $\delta \in \Omega \setminus \Delta$, and the point stabilizers of G are distinct maximal subgroups (G is clearly not regular), therefore $\Omega \setminus \Delta = \{\delta\}$ as claimed.

This shows that G is 2-transitive, and that G_δ, and hence every one-point stabilizer of G, acts primitively on its support. We can now proceed by induction on n. If $n \geq p + 4$ then the induction hypothesis applied to G_δ and x shows that $G_\delta \geq Alt(\Omega \setminus \{\delta\})$; hence G_δ contains a 3-cycle, and so $G \geq Alt(\Omega)$ by Theorem 3.3A. Thus consider the one remaining base case where $n = p + 3$. Since $p > 3$, $P := \langle x \rangle$ is a Sylow p-subgroup of G. Put $N := N_G(P)$, and note that $\Sigma := \mathrm{fix}(P)$ is N-invariant since $\Sigma^u = \mathrm{fix}(P^u) = \mathrm{fix}(P)$ for all $u \in N$.

We claim that $N^\Sigma = Sym(\Sigma) \cong S_3$. Indeed otherwise, $N_\alpha = N_{\alpha\beta}$ for two distinct points $\alpha, \beta \in \Sigma$. However N_α and $N_{\alpha\beta}$ are the normalizers of P in G_α and $G_{\alpha\beta}$, respectively. Hence the Sylow theorems (Exercises 1.4.12 and 1.4.13) and the 2-transitivity of G give the contradiction:

$$1 \equiv |G_\alpha : N_\alpha| = |G_\alpha : G_{\alpha\beta}|\,|G_{\alpha\beta} : N_{\alpha\beta}| \equiv n - 1 \pmod{p}.$$

This shows that $N^\Sigma = Sym(\Sigma\ )$ as claimed.

Finally, N acts by conjugation on P; the kernel of this action is $C := C_G(P)$ and the image of this action lies in $\mathrm{Aut}(P)$. Because P is cyclic, $\mathrm{Aut}(P)$ is abelian (Exercise 2.2.2), and so $N' \leq C$. Now a simple calculation shows that $C^{\Omega \setminus \Sigma} = \langle x \rangle$, and $C^\Sigma \geq (N')^\Sigma$ contains a 2-cycle from

above. Choose $y \in C$ such that y^Σ is a 2-cycle. Then $y^{\Omega\setminus\Sigma} \in \langle x \rangle$ and $p \neq 2$, so y^p is a 2-cycle in C. This shows that G contains a 2-cycle, and so $G \geq Alt(\Omega)$ by Theorem 3.3A. □

Exercises

3.3.16 Let H and K be subgroups of $Sym(\Omega)$ with supports Δ and Γ, respectively. If each of H and K acts primitively on its support, and $\Delta \cap \Gamma \neq \emptyset$, show that $\langle H, K \rangle$ acts primitively on $\Delta \cup \Gamma$.

3.3.17 Let C be the centralizer of a cycle x in $Sym(\Omega)$. If x has support Λ, show that $C^\Lambda = \langle x \rangle$. [*Hint:* Use Exercise 1.2.6.]

3.3.18 Show that the order of a proper primitive group of degree 19 cannot be divisible by 7. [Hint: If the Sylow 7-subgroup is nontrivial, show that its centralizer contains a 5-cycle.]

3.4 Frobenius Groups

A *Frobenius group* is a transitive permutation group which is not regular, but in which only the identity has more than one fixed point. Historically, finite Frobenius groups have played an important role in many areas in finite group theory, including the analysis of 2-transitive groups and finite simple groups. The present section gives a survey of some of the properties of these groups. Unfortunately, proofs of the basic structure theorems of finite Frobenius groups must be omitted because they require techniques such as character theory which would require a major diversion from our central theme.

EXAMPLE 3.4.1. Let U denote a subgroup of the group of units of a field F. Then the set G consisting of all permutations of F of the form

$$t_{\alpha\beta} : \xi \mapsto \alpha\xi + \beta \quad \text{with } \alpha \in U, \beta \in F$$

is a Frobenius group where the point stabilizer of 0 is

$$G_0 = \{t_{\alpha 0} \mid \alpha \in U\} \cong U.$$

The elements of G which fix no points, together with the identity, are the translations $t_{1\beta} : \xi \mapsto \xi + \beta$. These translations constitute a normal subgroup $K \cong (F, +)$ of G.

Let $G \leq Sym(\Omega)$ be a Frobenius group. Then $G_\alpha \cap G_\beta = 1$ for any two distinct points α, β in Ω, and so we say that the conjugacy class of stabilizers is a *trivial intersection set* (*TI-set*). The stabilizer G_α acts regularly on each of its orbits on $\Omega \setminus \{\alpha\}$. When Ω is finite, this implies that $|G_\alpha|$ divides $|\Omega| - 1$ and so G is quite a small subgroup of $Sym(\Omega)$. An important role

in the analysis of a Frobenius group is played by the set

$$K := \{x \in G \mid x = 1 \text{ or } \operatorname{fix}(x) = \emptyset\} \tag{3.2}$$

consisting of the identity and the elements of G not in any point stabilizer (the *fixed point free* elements). In the example above K is a normal subgroup of G, and as we shall see later this is always true when G is finite but not when G is infinite.

Exercises

Let $G \leq Sym(\Omega)$ be a Frobenius group with the set K defined as in (3.2).

3.4.1 Show that for each $u \neq 1$ in $K, C_G(u) \subseteq K$; and for each $x \neq 1$ in $G_\alpha, C_G(x) \leq G_\alpha$.

3.4.2 Show that the following are equivalent:
- (i) K is a subgroup of G;
- (ii) for some $\alpha \in \Omega$, distinct elements of K lie in distinct right G_α-cosets;
- (iii) for all $\alpha \in \Omega$, distinct elements of K lie in distinct right G_α-cosets.
- (iv) for all $\alpha, \beta \in \Omega$ there is at most one element $x \in K$ such that $\alpha^x = \beta$.

3.4.3 Suppose that $n := |\Omega| < \infty$. Show that each element in K has order dividing n, and that $|K| = n$.

3.4.4 Suppose that K is a subgroup of G. Show that K must be a normal subgroup. If Ω is finite, show that K is regular.

The structure of finite Frobenius groups has been described in major theorems of G. Frobenius, H. Zassenhaus and J.G. Thompson. However, since the proofs of these theorems would lead us too far away from the main theme of this book, they will be omitted. The interested reader will find expositions in the books of Huppert (1967), Passman (1968), and Tsuzuku (1982). The key result, part (i) below, is due to Frobenius (1902) and was an early triumph for techniques using character theory from the theory of linear representations. There is still no more elementary proof known. Part (ii) is from Zassenhaus (1936) while part (iii) is from Thompson (1959).

Structure Theorem for Finite Frobenius Groups. *Let G be a finite Frobenius group, G_α be a point stabilizer, and let*

$$K := \{x \in G \mid x = 1 \text{ or } \operatorname{fix}(x) = \emptyset\}.$$

- (i) *K is a subgroup of G (and so normal and regular by Exercise 3.4.4).*
- (ii) *For each odd prime p, the Sylow p-subgroups of G_α are cyclic, and the Sylow 2-subgroups are either cyclic or quaternion. If G_α is not solvable, then it has exactly one nonabelian composition factor, namely A_5.*
- (iii) *K is a nilpotent group.*

Exercises

3.4.5 Show that a primitive permutation group with abelian point stabilizers is either regular of prime degree or a Frobenius group.

3.4.6 Let G be a finite primitive permutation group with abelian point stabilizers. Use part (i) of the Structure Theorem to show that G has a regular normal elementary abelian p-subgroup for some prime p. [*Hint:* Exercise 1.4.14 may be helpful.] (It is also known that a finite primitive group with a nilpotent point stabilizer is solvable if the Sylow 2-subgroup of the stabilizer is nilpotent of class at most 2. See Janko (1964).)

3.4.7 If G is a finite group which contains a maximal subgroup M which is abelian, show that G is solvable and that $G^{(3)}$ (the third term in the derived series) equals 1.

The following two theorems give elementary proofs of parts of the Structure Theorem stated above in some special cases. Other special cases are considered in Burnside (1911, Sect. 134), Grün (1945) and Shaw (1952). Frobenius' theorem has been generalized in Wielandt (1958).

Theorem 3.4A. *Let $G \leq Sym(\Omega)$ be a finite Frobenius group of degree n, and let K be the set defined by (3.2). If G_α has even order, then K is a regular normal abelian subgroup of G and G_α has exactly one element of order 2.*

Proof. Since G_α has even order it contains an element of order 2. Let T be the G-conjugacy class containing this element. Since the point stabilizers of G are conjugate and disjoint, each of the n point stabilizers contains at least one element from T and $|T| \geq n$. Consider the cycle decomposition of an element $t \in T$: t has one cycle of length 1 and $(n-1)/2$ cycles of length 2. Since no nontrivial element of G has more than one fixed point, no two elements from G can contain the same 2-cycle. There are exactly $n(n-1)/2$ 2-cycles in $Sym(\Omega)$, and so we conclude that $|T|\,(n-1)/2 \leq n(n-1)/2$ and hence $|T| \leq n$. But $|T| \geq n$ from above, so $|T| = n$, and every 2-cycle occurs in one of the elements of T. In particular, each point stabilizer contains exactly one element from T, and T contains all elements of order 2 in G.

We now claim that $st \in K$ whenever $s,t \in T$. Suppose the contrary. Then $\text{fix}(st) = \{\beta\}$ for some $\beta \in \Omega$ and some distinct elements s and t from K. Then $\beta^t = \beta^{(st)t} = \beta^s$, and so either $(\beta\beta^s) = (\beta\beta^t)$ is a 2-cycle appearing in both s and t, or $\beta^s = \beta^t = \beta$ (and so $s,t \in G_\beta$). However, as we have seen above, neither of these cases is possible, and so we have a contradiction. Thus we conclude that $st \in K$ as claimed.

Fix $t \in T$. Then $Tt \subseteq K$, and since both sets have size n we conclude that $Tt = K$. In particular, $1 \in K$ and $KK^{-1} \subseteq TT \subseteq K$, so K is a subgroup; by Exercise 3.4.4 it is therefore a regular normal subgroup of G.

Finally, because each $u \in K$ has the form $u = st$ $(s \in T)$, we therefore have $t^{-1}ut = st = u^{-1}$ for each $u \in K$. But this means that for all $u, v \in K$, $uv = t^{-1}(uv)^{-1}t = t^{-1}(v^{-1}u^{-1})t = vu$. Hence K is abelian, and the proof is completed. □

Theorem 3.4B. *Let $G \leq Sym(\Omega)$ be a 2-transitive Frobenius group, and let K be the set defined by (3.2). Suppose that either: (i) G is finite; or (ii) the point stabilizers G_α are abelian. Then K is a regular normal abelian subgroup of G in which each nontrivial element has the same order.*

Remark. A 2-transitive Frobenius group is also known as a *sharply 2-transitive* group; further information about these groups is presented in Sect. 7.6. With respect to hypothesis (ii), we recall that Exercise 3.4.5 shows that a 2-transitive group with abelian point stabilizers is necessarily a Frobenius group.

PROOF. (i) Put $n := |\Omega|$. Then $|K| = n$ and $|G_\alpha|$ divides $n-1$, and hence $|G_\alpha| = n-1$ because G is 2-transitive. Suppose that $u \neq 1$ lies in K. Then $C_G(u) \subseteq K$ (see Exercise 3.4.1) and so $|G : C_G(u)| \geq n-1$. Hence u has at least $n-1$ conjugates in G. On the other hand, each conjugate of u is clearly a nontrivial element from K, so we conclude that: $C_G(u) = K$; u has $n-1$ conjugates in G; and these conjugates are precisely the nontrivial elements of K. Thus we have shown that K is a subgroup, each element of K lies in the centre of K, and all elements of K are conjugate. This can only happen when K is an elementary abelian p-group. Finally K is regular and normal by Exercise 3.4.4.

(ii) Let T be the set of all elements of order 2 in G. We claim that for every pair α, β of distinct points there is a unique $t \in T$ which maps α onto β. Indeed, 2-transitivity implies that there exists $t \in G$ such that $(\alpha, \beta)^t = (\beta, \alpha)$. Since G is a Frobenius group and t^2 fixes both α and β, we conclude that $t^2 = 1$ (and $t \neq 1$); thus $t \in T$. On the other hand, if $s \in T$ and $\alpha^s = \beta$, then $\beta^s = \alpha$ and so st^{-1} fixes two points and so must equal 1. Thus t is the unique element of T mapping α onto β.

Next note that if $s, t \in T$ and neither fixes α, then there exists $x \in G_\alpha$ such that $x^{-1}sx = t$. Indeed, by 2-transitivity we can choose $x \in G_\alpha$ such that $(\alpha, \alpha^s)^x = (\alpha, \alpha^t)$. Then $x^{-1}sx \in T$ and maps α onto α^t; hence $x^{-1}sx = t$ by the uniqueness proved above.

Also, there is at most one element of T in each G_α. For suppose that $s, t \in T \cap G_\alpha$. Then from above there exists $x \in G_\beta$ with $\beta \neq \alpha$ such that $x^{-1}sx = t$, and so $\alpha^x = \alpha^{sx} = \alpha^{xt}$. Since t only fixes one point, $\alpha = \alpha^x$, and hence x fixes both α and β. Thus $x = 1$, and $s = t$ as claimed.

Suppose now that x is any element of K and let $\beta := \alpha^x$. From what we have proved, there is a unique $t \in T$ such that $\alpha^{xt} = \alpha$. Then $xt \in G_\alpha$ so $\beta \neq \beta^{xt}$. We claim that either $x = t$ or $xt \in T$. Suppose that $xt \neq 1$.

There is a unique element $s \in T$ such that $(\beta, \beta^{xt})^s = (\beta^{xt}, \beta)$. Then $xts \in G_\beta$ and if $s \in G_\alpha$ then xts fixes 2 points and hence $xt = s \in T$. So suppose that $s \notin G_\alpha$. As we have shown above, there is an element $z \in G_\alpha$ such that $z^{-1}sz = t$. But xt and z are in G_α which is abelian, by hypothesis. Thus $xtsz = xtzt = zx$. So $\beta^{zx} = \beta^{xtsz} = \beta^z$ and the element $x \in K$ has the fixed point β^z, a contradiction. Therefore $s \in G_\alpha$ and $xt = s \in T$.

Suppose that K is not a subgroup. Then Exercise 3.4.2 shows that there must exist distinct nontrivial $x, y \in K$ such that $xy^{-1} \in G_\alpha$. Then, with $\beta := \alpha^x = \alpha^y$ there is a unique element $t \in T$ such that $\beta^t = \alpha$. The argument above shows that either $x = y = t$ or else xt and yt are each elements of $T \cap G_\alpha$, contrary to what we have shown above. □

If G is a 2-transitive Frobenius group with abelian stabilizers G_α as considered in part (ii) of Theorem 3.4B, then G is a one-dimensional affine group $AGL_1(F)$ over some (commutative) field F (see Corollary 7.6A).

Exercises

The object of this set of exercises is the construction of a finite Frobenius group with a nonabelian regular normal subgroup; part (iii) of the Structure Theorem for Finite Frobenius Groups, shows that the subgroup must be nilpotent. Let q be a prime power and n be an odd integer, and let F be a field of order q^n. Put $\Omega := F \times F$. Since the group of units of F is cyclic of order $q^n - 1$, it contains a unique (cyclic) subgroup U of order $(q^n - 1)/(q - 1)$. Let σ be the automorphism of F defined by $\sigma(\xi) := \xi^{q^{(n+1)/2}}$.

3.4.8 For all $\alpha, \beta \in F$, define $g_{\alpha\beta} : (\xi, \eta) \mapsto (\xi + \alpha, \eta + \beta + \xi\sigma(\alpha))$. Show that each $g_{\alpha\beta}$ is a permutation of Ω, and that the set K of all such permutations is a regular subgroup of $Sym(\Omega)$.

3.4.9 For each $\gamma \in U$, define $h_\gamma : (\xi, \eta) \mapsto (\gamma\xi, \gamma\sigma(\gamma)\eta)$. Show that each h_γ is a permutation of Ω, and the set H of all such permutations is a subgroup of $Sym(\Omega)$ which normalizes K.

3.4.10 Show that $G := KH$ is a Frobenius group with a nonabelian regular normal subgroup K. (The case $q = 2$ gives a Frobenius group of degree 2^{2n} and order $2^{2n}(2^n - 1)$ which occurs as the point stabilizer of a 2-transitive group called the Suzuki group $Sz(2^n)$; this group is discussed further in Sect. 7.7.)

Exercises

The object of this set of exercises is to give a construction of a finite Frobenius group with a nonsolvable point stabilizer; part (ii) of the Structure Theorem for Finite Frobenius Groups shows that A_5 is the only nonabelian composition factor which can arise. Let F be a finite field whose characteristic is not 2, 3 or 5 and such that for some $\alpha, \beta \in F$ we have $\alpha^2 = -1$

and $\beta^2 + \beta = 1$. Consider the subgroup H of $SL_2(F)$ generated by

$$x := \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, y := \begin{bmatrix} 0 & \alpha \\ \alpha & \beta \end{bmatrix} \text{ and } z := \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

3.4.11 Show that a field of size 29 has the required properties.

3.4.12 Show that $x^3 = y^5 = 1$, and that $(xy)^2 = z$. Hence prove that $H/\langle z\rangle \cong A_5$.

3.4.13 Let G be the group of all permutations of F^2 of the form

$$x_{u\gamma\delta} : (\xi, \eta) \mapsto (\xi, \eta)u + (\gamma, \delta)$$

where $u \in H$ and $\gamma, \delta \in F$. Show that G is a Frobenius group whose point stabilizers are isomorphic to H.

The structure theorem for finite Frobenius groups which is stated above does not carry over to infinite Frobenius groups. The following examples show how badly it fails. Let $G \leq Sym(\Omega)$ be an infinite Frobenius group and let $K := \{x \in G \mid x = 1 \text{ or fix}(x) = \emptyset\}$.

EXAMPLE 3.4.2. (An example where K is not a subgroup) Let F be the free group on generators x, y and put $z := [x, y]$. If $w \in F$, then $w^{-1}zw \in H := \langle z\rangle$ occurs only if $w \in H$ (see Exercise 3.4.14). Let Ω be the set of subgroups conjugate to H in F. Then F acts faithfully (and transitively) on Ω by conjugation; let $G \cong F$ be the image of this action. By the observation above, each $w \neq 1$ in the point stabilizer F_H lies in H and so cannot fix any other point of Ω. Thus G is a Frobenius group. On the other hand, every conjugate of H is contained in the derived group F', and so K contains all elements in $G \setminus G'$. Since $K \neq G$, this shows that K is not a subgroup of G.

EXAMPLE 3.4.3. (An example where $K = 1$) For sufficiently large primes p, the Burnside groups $B(m, p)$ with $m \geq 2$ are infinite simple groups in which every proper nontrivial subgroup has order p, and all subgroups of order p are conjugate [see Adian (1979)]. Let G be the image of such a group acting by conjugation on the set Ω of its subgroups of order p. Then G is a Frobenius group in which there are no fixed-point-free elements.

EXAMPLE 3.4.4. (An example where K is a regular normal subgroup, but K is not nilpotent) Let S be a group and consider the set T of all doubly infinite sequences $\{s_i\}_{i\in\mathbb{Z}}$ with $s_i \in S$ with all but a finite number of s_i equal to 1. This is a group under componentwise multiplication. Let K be the image of the regular representation of T in $Sym(\Omega)$ where $\Omega = T$. Since $z : \{s_i\} \mapsto \{s_{i+1}\}$ defines an automorphism of T, the element z lies in the normalizer of K in $Sym(\Omega)$ (compare with Exercise 2.5.6); we define $G := \langle K, z\rangle$. The point stabilizer G_1 equals $\langle z\rangle$, and it is clear that each nonidentity element of $\langle z\rangle$ has 1 as its unique fixed point. Thus G is

a Frobenius group. The nontrivial elements of K are precisely the fixed-point-free elements of G. Moreover K is a regular normal subgroup which is not nilpotent provided S is not nilpotent.

Exercises

3.4.14 Let F be a free group on generators x and y. If $w \neq 1$ is in F, show that the normalizer N of $\langle w \rangle$ in F is equal to the centralizer of $\langle w \rangle$. If $w := [x, y]$, show that $N = \langle w \rangle$. (Note that if $w = x^2$ then $N \neq \langle w \rangle$.)

3.4.15 Show that the group G in Example 3.4.3 is not 2-transitive. Is it primitive?

3.4.16 Show that the group G in Example 3.4.4 is not primitive. Does it have minimal blocks of imprimitivity?

3.5 Permutation Groups Which Contain a Regular Subgroup

A permutation group which contains a regular subgroup is clearly transitive. Conversely, a subgroup R of a transitive group G is regular if and only if $G = G_\alpha R = RG_\alpha$ and $R \cap G_\alpha = 1$ for each point stabilizer G_α. Thus the existence of a regular subgroup for G implies a group structure on a particular set R of coset representatives for a point stabilizer. This extra structure can be used to derive some useful theorems about such groups. The earliest of these theorems was due to W. Burnside who considered transitive groups of prime degree. If G is a transitive group of prime degree p, then G necessarily contains a p-cycle, and this p-cycle generates a regular subgroup which is a Sylow p-subgroup of G. Burnside proved that either G is 2-transitive or G has a normal Sylow p-subgroup. Burnside's original proof used character theory, but a number of other proofs have since been discovered. At the end of this section we shall give a proof, due to I. Schur, of Burnside's result.

Exercise

3.5.1 Let G be a transitive permutation group of prime degree p. Show that the following are equivalent:
   (i) G is solvable;
   (ii) G has a normal Sylow p-subgroup; and
   (iii) G is permutation isomorphic to a subgroup of the affine group $AGL_1(p)$ (see Sect. 2.8).

If G is a permutation group containing a normal regular subgroup R, then G is contained in the holomorph of R (see Exercise 2.5.6) and in some sense is "known". The more interesting case is where R is not normal. A

striking example where G is infinite is given by the automorphism group of the countable universal graph (see Chap. 9) which has $2^{\aleph_0}$ conjugacy classes of regular subgroups. The following construction gives examples of finite groups with nonnormal regular cyclic subgroups.

EXAMPLE 3.5.1. Let E be field with q^d elements where q is a prime power and $d > 1$. The group of units of E is a cyclic group generated by some element γ, say. The field E contains a subfield F of size q, and E is a vector space of dimension d over F. Consider the group $G := GL_F(E) \cong GL_d(F)$ of all invertible F-linear transformations of E into itself. Then G acts on the set $\Omega := E \setminus \{0\}$, and the element $u : \xi \mapsto \xi\gamma$ of order $q^d - 1$ in G generates a subgroup R which acts regularly on Ω. It is readily seen that R is not normal in G. The action of G on Ω is not primitive. The set $\overline{\Omega}$ of lines is a system of blocks, and the image $\overline{G}$ of the action of G on $\overline{\Omega}$ is the projective group $PGL_F(E) \cong PGL_d(q)$ (see Sect. 2.8). The image $\overline{R}$ of R in this action is again a regular cyclic subgroup (sometimes called a *Singer cycle*). In this case $\overline{G}$ is a 2-transitive group.

In Example 3.5.1 we gave two types of groups containing a nonnormal regular cyclic subgroup: an imprimitive group and a 2-transitive group. As we shall see (Theorems 3.5A and Corollary 3.5B), these are essentially the only two possibilities; any finite primitive group containing a nonnormal regular cyclic subgroup must be 2-transitive.

Our study of groups with regular subgroups begins with the following observation. Suppose that $G \leq Sym(\Omega)$ has a regular subgroup R, and let G_α be a point stabilizer of G. Then R is a set of right coset representatives of G_α in G, and so there exists a uniquely determined function $\phi : G \to Sym(R)$ such that $G_\alpha u^{\phi(x)} = G_\alpha ux$ for all $u \in R$ and $x \in G$. A simple calculation shows that ϕ defines a permutation isomorphism of G onto a subgroup of $Sym(R)$.

Exercise

3.5.2 Show that ϕ defines a permutation isomorphism of G onto $\mathrm{Im}(\phi)$. Moreover, $u^{\phi(x)} = ux$ whenever both u and x lie in R, so $\phi(R)$ is the image of the regular representation of R in $Sym(R)$.

A consequence of the observation above is that, in studying permutation groups with regular subgroups, it is enough to look at subgroups of $Sym(R)$ which contain the image of the regular representation of R. We can exploit this extra group structure on the underlying set R by using a group ring. Let H be a finite group and F be an arbitrary field, and consider the set $F[H]$ of all formal sums $\sum_{u \in H} \lambda_u u$ with coefficients $\lambda_u \in F$. Addition and multiplication are defined on $F[H]$ by

$$\sum_{u \in H} \lambda_u u + \sum_{u \in H} \mu_u u := \sum_{u \in H} (\lambda_u + \mu_u) u$$

and

$$\left(\sum_{u\in H} \lambda_u u\right)\left(\sum_{u\in H} \mu_u u\right) := \sum_{u\in H} \nu_u u \quad \text{where } \nu_u := \sum_{v\in H} \lambda_v \mu_{v^{-1}u}.$$

Under these operations $F[H]$ is a ring (see Exercise 3.5.3 below) whose group of units contains a copy of H; we identify the element v in H with the ring element $\sum_{u\in H} \lambda_u u$ where $\lambda_u = 1$ when $u = v$ and $\lambda_u = 0$ otherwise. Since $F[H]$ contains a copy $\{\lambda 1 \mid \lambda \in F\}$ of F, the ring $F[H]$ is also a vector space of dimension $|H|$ over F; indeed it is an F-algebra. We call $F[H]$ the *group ring* of H over F.

Exercise

3.5.3 Show that $F[H]$ is indeed a ring with these operations, and that $F[H]$ is a vector space over F with the set of elements of H as a basis.

In the case that R is a finite group and the group G acts on R, we can extend the action of G on R to an action on the group ring $F[R]$ via:

$$\left(\sum_{u\in R} \lambda_u u\right)^x := \sum_{u\in R} \lambda_u (u^x).$$

This action of G is linear in the sense that it respects the vector space properties of $F[R]$ although it does not, in general, respect the multiplication in $F[R]$.

We define the *support* of $c := \sum_{u\in R} \lambda_u u \in F[R]$ by

$$\mathrm{supp}(c) := \{u \in R \mid \lambda_u \neq 0\} \subseteq R.$$

Clearly, $\mathrm{supp}(c)$ is invariant under $x \in G$ whenever c is fixed by x (the converse is not usually true).

In our computations below we shall frequently use the following elementary fact. Suppose that S is a ring with unity 1 with characteristic p for some prime p (so $1 + 1 + \ldots + 1(p \text{ summands}) = p1$ equals 0 in S). Then, whenever $a_1, \ldots, a_k \in S$ commute pairwise, we have $(a_1 + \ldots + a_k)^p = a_1 + \ldots + a_k$.

Exercise

3.5.4 Prove the previous statement. [*Hint:* First prove that p divides each of the binomial coefficients $\binom{p}{i}$ for $i = 1, \ldots, p-1$.]

Suppose that R is a finite group and that the group $G \leq Sym(R)$ contains the regular representation of R. Let F be an arbitrary field and let $C(G_1)$ denote the set of fixed points of G_1 in $F[R]$. The next lemma shows that this subset of the group ring is actually a subring. The ring $C(G_1)$, sometimes called a *Schur ring*, plays a central role in the analysis to follow.

Lemma 3.5A. *Suppose that R is a finite group and that $G \leq Sym(R)$. Let $\Delta_1 = \{1\}, \Delta_2, \ldots, \Delta_r$ be the orbits in R of the point stabilizer G_1. Then:*

(i) *$\mathcal{C}(G_1)$ is a vector subspace of $F[R]$, and the elements $c_i := \sum_{u \in \Delta_i} u$ for $i = 1, \ldots, r$ form an F-basis for $\mathcal{C}(G_1)$;*

(ii) *$\mathcal{C}(G_1)$ is a subring (and hence a subalgebra) of $F[R]$.*

PROOF. (i) Let $c := \sum_{u \in R} \lambda_u u$. Then $c \in \mathcal{C}(G_1) \iff c = c^x$ for all $x \in G_1 \iff \lambda_u = \lambda_v$ whenever u and v lie in the same G_1 -orbit $\iff c$ is an F-linear combination of $c_1, \ldots, c_r$. Since the c_i are clearly linearly independent, the result follows.

(ii) We begin by proving the following identity:

(3.3) If $\Gamma \subseteq R$ is G_1-invariant, then $(\Gamma u)^x = \Gamma u^x$ for all $u \in R$, $x \in G_1$.

Indeed, $G_1 ux = G_1 u^x$ and so, for some $y \in G_1$, we have $ux = yu^x$. Hence for all $v \in \Gamma$ we have $G_1(vu)^x = G_1 v(ux) = G_1 vyu^x = G_1 v^y u^x$, and hence $(vu)^x = v^y u^x$. Since Γ is G_1-invariant, v^y runs over Γ as v runs over Γ, and therefore $(\Gamma u)^x = \Gamma u^x$ as claimed.

Now $\mathcal{C}(G_1)$ is a vector space with a basis $c_1, \ldots, c_r$ by (i), so to prove that $\mathcal{C}(G_1)$ is a ring it is enough to show that $c_i c_j \in \mathcal{C}(G_1)$ for all i and j. Fix $x \in G_1$. Then (3.3) shows that $(\Delta_i u)^x = \Delta_i u^x$ for all $u \in \Delta_j$; hence summing over Δ_i gives $(c_i u)^x = c_i u^x$. Now summing over all $u \in \Delta_j$ gives $(c_i c_j)^x = c_i c_j$ since u^x runs over Δ_j as u runs over Δ_j. This is true for each $x \in G_1$ and so $c_i c_j$ is fixed by G_1 as required. □

Exercise

3.5.5 Show that for any two G_1-invariant subsets Γ, Δ of R, the subset $\Gamma\Delta$ is also G_1-invariant.

Lemma 3.5B. *Under the hypothesis of Lemma 3.5A suppose that R has order n, and that G contains the image of the regular representation of R. For each integer k, define $\Delta_i(k) := \{u^k \mid u \in \Delta_i\}$ for $i = 1, \ldots, r$.*

(i) *G is a primitive group $\iff$ for each $c \in \mathcal{C}(G_1)$ the subgroup $\langle \mathrm{supp}(c) \rangle$ of R generated by the support of c is either 1 or R.*

(ii) *If R is abelian, and k is relatively prime to n, then the mapping $\Delta_i \mapsto \Delta_i(k)$ defines a permutation of the set of G_1-orbits in R.*

(iii) *Suppose that G is primitive, R is abelian, and p is a prime dividing n. Let Γ be a G_1-invariant subset of R, and put $c := \sum_{u \in \Gamma} u \in F[R]$ where F is a field of characteristic p. Then $c^p = m1$ where m is the number of elements $u \in \Gamma$ with $u^p = 1$.*

PROOF. (i) The blocks containing 1 for the regular representation of R (acting on R) are just the subgroups of R. Hence $\Gamma \subseteq R$ is a block containing 1 for G if and only if Γ is a subgroup of R and is G_1-invariant. Thus, if G is imprimitive, then there exists a subgroup Γ such that $1 < \Gamma < R$

and that Γ is G_1-invariant. In this case, $c := \sum_{u\in\Gamma} u \in \mathcal{C}(G_1)$ and $\langle \mathrm{supp}(c)\rangle = \Gamma \neq 1$ or R. Conversely, suppose there exists $c \in \mathcal{C}(G_1)$ with support Δ such that $\Gamma := \langle\Delta\rangle \neq 1$ or R; then $\Gamma = \cup_{i=0}^{n}\Delta^i$, and so Γ is G_1-invariant by Exercise 3.5.5. Thus Γ is a G_1-invariant subgroup of R, and so G is imprimitive.

(ii) We shall first prove the result when $k = p$ is a prime with $p \not| \ n$. Choose $F = \mathbb{F}_p$ as the field with p elements. Then the remarks preceding Lemma 3.5A show that $c_i^p = \sum_{u\in\Delta_i} u^p$ for each i because R is abelian, and no two terms in the sum are equal because $p \not| \ |R|$. Now $\Delta_i(p) = \mathrm{supp}(c_i^p) \in \mathcal{C}(G_1)$ by Lemma 3.5A(ii). Since $p \not| \ n$, the mapping $u \mapsto u^p$ is a bijection of R onto itself, so $\Delta_i(p)$ $(i = 1, \dots, r)$ is a partition of R into r (nonempty) G_1-invariant subsets. Since G_1 has r orbits on R, these subsets must be precisely the orbits of G_1. This proves the result in the special case where $k = p$ is prime.

For the general case, choose $m > 0$ with $m \equiv k \bmod n$. Then successive applications of the special case above to the prime factors of m shows that $\Delta_i \mapsto \Delta_i(m)(= \Delta_i(k))$ is a permutation of the orbits of G_1.

(iii) Since Γ is G_1-invariant, $c \in \mathcal{C}(G_1)$. Also, by the remark preceding Lemma 3.5A, $c^p = \sum_{u\in\Gamma} u^p$. Since p divides $|R|$ and R is abelian, the index of $\langle\mathrm{supp}(c^p)\rangle$ in R is divisible by p. Now (i) and the primitivity of G show that $\mathrm{supp}(c^p) \subseteq \{1\}$, and $c^p = m1$ as asserted. □

Theorem 3.5A. *Let G be a permutation group of degree n containing a regular subgroup R. Suppose that R is abelian and has a cyclic Sylow p-subgroup for some prime p with $p < n$. Then G is either imprimitive or 2-transitive.*

PROOF. As we noted at the beginning of this section, it is enough to consider the case where G is a subgroup of $Sym(R)$ containing the image of the regular representation of R. By hypothesis, R is abelian and has a unique subgroup P of order p. We shall assume that G is primitive, and prove that the orbits of G_1 on R are $\{1\}$ and $R\setminus\{1\}$ (so G is 2-transitive). We do this by a series of calculations in the group ring $\mathbb{F}_p[R]$.

We first show that each G_1-orbit $\Gamma \subseteq R$ contains at least one element from P, and that the subset $\Gamma \setminus P$ of remaining elements is a union of complete cosets of P. To prove this, consider $c := \sum_{u\in\Gamma} u \in \mathbb{F}_p[R]$. Then $c \in \mathcal{C}(G_1)$ and Lemma 3.5B (iii) shows that $c^p = \sum_{u\in\Gamma} u^p = |\Gamma \cap P|\,1$. This shows that, if $u \in \Gamma \setminus P$ (so $u^p \neq 1$), then the number of elements $v \in \Gamma$ such that $v^p = u^p$ must be a multiple of p. Since R is abelian, $v^p = u^p \iff (vu^{-1})^p = 1 \iff vu^{-1} \in P$; hence $u \in \Gamma\setminus P$ implies that the whole coset $Pu \subseteq \Gamma$. This shows that $\Gamma\setminus P$ is a union of complete cosets of P. We now show that $\Gamma \cap P \neq \emptyset$. Indeed, otherwise, Γ itself is a complete union of cosets of P, and so $P \subseteq H := \{u \in R \mid \Gamma u = \Gamma\}$. Clearly H is a (nontrivial) subgroup of R, and H is G_1-invariant by (3.3). Now Lemma 3.5B (i) shows that $H = R$ because we are assuming G is

primitive. But this implies that $R = \Gamma R = \Gamma$ which is impossible because there are at least two G_1-orbits in R. Hence $\Gamma \cap P \neq \emptyset$ as asserted.

Now suppose that G is not 2-transitive. Then there exists a G_1-orbit Γ not containing 1 such that $m := |\Gamma \cap P| \leq (p-1)/2$, and $m > 0$ by what we have just proved. Define $a := \sum_{u \in \Gamma \cap P} u$, $b := \sum_{u \in P} u$, and $c := \sum_{u \in \Gamma} u$ in $\mathbb{F}_p[R]$. Then, from what we have just proved, $c = a + bd$ where $d \in \mathbb{F}_p[R]$ is a sum of certain coset representatives for P in R. Moreover, if $v \in P$, then $Pv = P$, and so $bv = b$; hence $ab = mb$ and $b^2 = |P|\, b = 0$. Since $c - m1 \in \mathcal{C}(G_1)$, therefore $e := (c - m1)^2 \in \mathcal{C}(G_1)$ by Lemma 3.5A (ii). On the other hand

$$e = (a - m1 + bd)^2 = (a - m1)^2 + 2(a - m1)bd + b^2d^2 = (a - m1)^2$$

which shows that $\mathrm{supp}(e) \subseteq P$. Since $P \neq R$ by hypothesis, and G is primitive, Lemma 3.5B (i) shows that $\mathrm{supp}(e) \subseteq \{1\}$; hence $(a - m1)^2 = \lambda 1$ for some $\lambda \in \mathbb{F}_p$. But the condition $m = |\Gamma \cap P| \leq (p-1)/2$ shows that the coefficient in $(a - m1)^2 = a^2 - 2ma + m^2 1$ of each $u \neq 1$ from $\Gamma \cap P$ must be nonzero. Thus we conclude that $\Gamma \cap P \subseteq \{1\}$. Since $1 \notin \Gamma$ by the choice of Γ, we arrive at a contradiction to the fact that $m = |\Gamma \cap P| > 0$. This contradiction shows that G must be 2-transitive as claimed. □

Exercise

3.5.6 Show that every finite elementary abelian p-group is isomorphic to a regular subgroup of some primitive group which is not 2-transitive.

A group B is called a *B-group* (after Burnside) if a primitive group containing a regular subgroup isomorphic to B is necessarily 2-transitive; Theorem 3.5A describes one class of B-groups. In fact B-groups are quite common. It was shown by Cameron et al. (1982) that for "most" values of n the only primitive subgroups of S_n are A_n and S_n; for these values of n, any group of order n is trivially a B-group. On the other hand, Exercise 3.5.6 shows that finite elementary abelian p-groups are not B-groups, and Exercise 4.7.11 will show that the direct product of six copies of A_5 is not a B-group. For infinite groups, Cameron and Johnson (1987) have given quite general constructions of primitive groups which contain a prescribed countable regular subgroup and which are not 2-transitive.

We now turn to the original case considered by Burnside where the group has prime degree p. In this case it is more convenient to take the set on which G acts as the field $\mathbb{F}_p$: $G \leq Sym(\mathbb{F}_p)$ and $R \leq G$ is the image of the regular representation of the *additive* group $(\mathbb{F}_p, +)$.

Now permutations of $\mathbb{F}_p$ are just functions with domain and range equal to $\mathbb{F}_p$, so consider the set $\mathcal{F}$ of all functions of $\mathbb{F}_p$ into itself. Since each of the p points in $\mathbb{F}_p$ has p potential images, $|\mathcal{F}| = p^p$. One way to construct elements of $\mathcal{F}$ is to use polynomial functions. Each polynomial $f(X) \in \mathbb{F}_p[X]$ defines a function $\xi \mapsto f(\xi)$ in $\mathcal{F}$, and two polynomials $f(X)$ and $g(X)$ define the same function if and only if $f(X) \equiv g(X) \bmod X^p - X$ (see

Exercise 3.5.7). In particular, each polynomial function is represented by a unique polynomial of degree $< p$. This means that there are exactly p^p different polynomial functions, and so each element of $\mathcal{F}$ is, in fact, a polynomial function (see also Exercise 3.5.8). In particular, each permutation in $Sym(\mathbb{F}_p)$ can be represented by exactly one polynomial of degree $< p$. Group multiplication is represented by composition followed by reduction modulo $X^p - X$ (take care with the order of composition).

Exercises

Let F be a finite field with q elements.

3.5.7 Show that $X^q - X = \prod_{\alpha \in F}(X - \alpha)$. Use this to show that two polynomials $f(X)$ and $g(X)$ over F define the same polynomial function of F into itself if and only if $f(X) \equiv g(X)(\mathrm{mod} X^q - X)$. [*Hint:* Every unit in F has order dividing $q - 1$.]

3.5.8 (Lagrange interpolation) Let ϕ be an arbitrary function from F into itself. Show that $f(X) := -\sum_{\alpha \in F} \phi(\alpha) \frac{(X^q - X)}{(X - \alpha)}$ is the unique polynomial of degree $< q$ such that $f(\alpha) = \phi(\alpha)$ for all $\alpha \in F$.

3.5.9 (L.E. Dickson's criterion) Show that a polynomial $f(X) \in F[X]$ represents a permutation of F if and only if $f(X)$ has a unique root in F and, for each integer m with $1 \leq m < q - 1$ and $\mathrm{GCD}(m, q) = 1$, the polynomial $f(X)^m$ is congruent $\mathrm{mod}\, X^q - X$ to a polynomial of degree $< q - 1$. (There is a considerable literature on "permutation polynomials".)

3.5.10 (Taylor expansion) Suppose that $f(X) \in F[X]$ has degree $d < p :=$ char F. Show that

$$f(X + Y) = f(X) + Yf^{(1)}(X) + \frac{Y^2}{2!} f^{(2)}(X) + \ldots + \frac{Y^d}{d!} f^{(d)}(X)$$

where $f^{(i)}(X)$ denotes the formal *ith* derivative of $f(X)$. (If $d \geq p$, the formula needs modification since then we cannot divide by $d!$ in F.)

With these ideas in hand, we are in a position to prove Burnside's theorem.

Theorem 3.5B. *Let G be a subgroup of $Sym(\mathbb{F}_p)$ containing the p-cycle $u_1 : \xi \mapsto \xi + 1$. Then G is either 2-transitive or $G \leq AGL_1(p)$.*

PROOF. The hypothesis is equivalent to the condition that G contains the regular representation $R = \{u_\alpha \mid \alpha \in \mathbb{F}_p\}$ of $(\mathbb{F}_p, +)$ where $u_\alpha : \xi \mapsto \xi + \alpha$. As we have seen above, each element of G can be represented by a polynomial of degree $< p$, and the elements of $AGL_1(p)$ are precisely the permutations represented by polynomials of degree ≤ 1. Thus, assuming that G is not 2-transitive, we have to show that each element of G is represented by a polynomial of degree at most 1.

Let Γ be the orbit containing 1 for the point stabilizer G_0 (recall that G is acting on the additive group $(\mathbb{F}_p, +)$). Translating to additive notation, Lemma 3.5B (ii) shows that $k\Gamma$ is also an orbit for G_0 for each integer k relatively prime to p; hence $\alpha\Gamma$ is an orbit for all $\alpha \neq 0$ in $\mathbb{F}_p$. In particular, this shows that Γ is closed under multiplication, and so Γ is a subgroup of the group of units of $\mathbb{F}_p$, and the other orbits of G_0 are just the cosets of Γ in this group of units. Because G is not 2-transitive, $h := |\Gamma|$ is a proper divisor of $p - 1$, and so $h < p/2$. On the other hand, because G contains a p-cycle, it is primitive. If G is regular, then certainly $G \leq AGL_1(p)$, so we may assume G is not regular and hence $h > 1$ (Exercise 1.6.5).

We next note two simple facts which we shall need. Firstly, let $x \in G_0$ and $\alpha \in \mathbb{F}_p$. Suppose that $\alpha^x = \beta$, and put $y := u_\alpha x u_\beta^{-1}$. Then y maps

$$\xi \mapsto \xi + \alpha \mapsto (\xi + \alpha)^x \mapsto (\xi + \alpha)^x - \beta = (\xi + \alpha)^x - \alpha^x.$$

Thus $0^y = 0$; so $y \in G_0$ and permutes the elements of Γ among themselves. Secondly, since the group of units of a finite field is cyclic, Γ is also a cyclic group, generated by γ, say. Hence, for each integer r, we have

$$(3.4) \qquad \sum_{\xi \in \Gamma} \xi^r = \sum_{i=0}^{h-1} \gamma^{ir} = \begin{cases} \frac{(\gamma^{rh}-1)}{(\gamma^r-1)} = 0 & \text{if } h \not| r \\ h & \text{if } h | r \end{cases}$$

Now consider a fixed $x \in G_0$, and let $f(X) \in \mathbb{F}_p[X]$ be the polynomial of degree $d < p$ such that $\xi^x = f(\xi)$ for all $\xi \in \mathbb{F}_p$. We shall show that $d = 1$.

The element y above permutes the elements of Γ, so for each $\alpha \in \mathbb{F}_p$ and each $r \geq 0$:

$$\sum_{\xi \in \Gamma} f(\xi + \alpha)^r = \sum_{\xi \in \Gamma} \{f(\xi + \alpha) - f(\alpha) + f(\alpha)\}^r = \sum_{\xi \in \Gamma} \{\xi + f(\alpha)\}^r.$$

This relationship between polynomial functions gives an identity between polynomials when the degrees are small enough. Specifically

$$\sum_{\xi \in \Gamma} f(\xi + X)^r = \sum_{\xi \in \gamma} \{\xi + f(X)\}^r \quad \text{whenever } dr = \deg f(X)^r < p.$$

Now applying the binomial theorem and using (3.4) gives

$$(3.5) \qquad \sum_{\xi \in \Gamma} f(\xi + X)^r = hf(X)^r \quad \text{provided } 1 \leq r < h \text{ and } dr < p.$$

On the other hand, we can expand any polynomial $g(X)$ of degree $k < p$ over $\mathbb{F}_p$ in a Taylor series:

$$g(\xi + X) = g^{(0)}(X) + \xi g^{(1)}(X) + \ldots + \xi^k g^{(k)}(X)/k!$$

where $g^{(i)}(X)/i!$ is a polynomial of degree $k - i$ (see Exercise 3.5.10). Therefore, putting $g_r(X) := f(X)^r$, equations (3.5) and (3.4) yield

$$h \sum_{0 \le i \le dr/h} g_r^{(hi)}(X)/(hi)! = hg_r(X) \quad \text{provided } dr < p \text{ and } 1 \le r < h.$$

Since the polynomials $g_r^{(hi)}(X)$ are linearly independent over $\mathbb{F}_p$ for $i = 0, \ldots, \lfloor dr/h \rfloor$, we deduce from this last equation that

(3.6) $\qquad dr < p$ and $1 \le r < h$ together imply that $dr/h < 1$.

Finally, taking $r = 1$ in (3.6) we see that $d < h$. Then, choosing $r > 1$ such that $d(r-1) < h \le dr$, we have $dr < h + d < p$ because $h < p/2$. Since $dr/h \ge 1$, (3.6) shows that $r \ge h$. This implies that $d(h-1) < h$. Since $h > 1$, $d = 1$ as required. □

Since a transitive permutation group of prime degree p contains a p-cycle, we get the following immediate corollary (see Exercise 3.5.1).

Corollary 3.5B. *Every transitive permutation group of prime degree p is either 2-transitive or is solvable with a regular normal Sylow p-subgroup.*

As early as 1832, E. Galois showed that the groups $PSL_2(p)$ have permutation representations of degree p when $p = 5, 7$ and 11, and in 1861 E. Mathieu discovered his important multiply transitive groups which include two groups of prime degree. Using the classification of finite simple groups, it is possible to obtain a complete list of the finite 2-transitive permutation groups (see Sect. 7.7), and hence the transitive groups of prime degree. The classification implies that any transitive group of prime degree p must be one of the following:

(i) the symmetric group S_p or the alternating group A_p;
(ii) a subgroup of $AGL_1(p)$;
(iii) a permutation representation of $PSL_2(11)$ of degree 11;
(iv) one of the Mathieu groups M_{11} or M_{23} of degree 11 or 23, respectively;
(v) a projective group G with $PSL_d(q) \le G \le P\Gamma L_d(q)$ of degree $p = (q^d - 1)/(q - 1)$.

Two of the examples of Galois ($PSL_2(p)$ with $p = 5$ and 7) are concealed in this list: $PSL_2(5) \cong A_5$, and $PSL_2(7) \cong PSL_3(2)$. The Mathieu groups are discussed in Chap. 6. The action in (iii) is described in Example 7.5.2. It is conjectured that there are infinitely many primes p of the form described in (v) (for example, every Mersenne prime has this form), but this has not been proved.

Exercises

3.5.11 Let $q = r^m$ be a power of a prime r. Show that necessary conditions for $(q^d - 1)/(q - 1)$ to be prime are: d is prime, $d \nmid q - 1$, and m is

a power of d. Use this to find all the primes $p < 100$ for which there are groups of the type (v) just described.

3.5.12 Let $G \leq S_n$ have odd order. If G contains an n-cycle, show that G is solvable.

3.6 Computing in Permutation Groups

The object of this section is to give a short outline of some techniques which are used in computing with permutation groups. Most of these techniques have been developed over the past 30 years, and are used, for example, by systems such as GAP, MAGMA (which incorporates the earlier system CAYLEY), MAPLE and MATHEMATICA to carry out computations in group theory. We shall outline the mathematical ideas behind these programs, but not give details of their implementation. Although the latter details are essential for efficient implementation and are often of interest in themselves, they lie outside the objectives of this book. Anyone seriously interested in carrying out computations with permutation groups should investigate the availability of one of the systems referred to above, particularly one of GAP or MAGMA which are dedicated to computations in group theory and related areas.

Given a permutation group $G \leq Sym(\Omega)$ on a finite set Ω, some natural questions which arise are:

- Order Problem: what is the order of G?
- Membership Problem: given $x \in Sym(\Omega)$, decide whether $x \in G$.
- Orbit Problem: what are the orbits of G?
- Block Problem: is G primitive? If not, find a nontrivial block for G.

A brief thought about these problems immediately raises the question as to how the group G is to be described. In mathematical problems, permutation groups may be described in many different ways, but in computational work it turns out that it is important to have a uniform description, and this is frequently chosen to be a set W of permutations generating G. In cases where an alternative description is given, for example, a definition of G as the automorphism group of a geometric structure, a preliminary step is carried out to construct a set of permutations generating G.

From here on we assume that $G \leq Sym(\Omega)$ and that W is a set of generators of G. Of the questions posed above, the easiest to deal with turn out to be those dealing with orbits and blocks.

(A) Computing Orbits

Consider the digraph $\mathcal{G}$ whose vertex set is Ω and whose edges are precisely the pairs (α, α^x) for all $\alpha \in \Omega$ and all $x \in W$ with $\alpha \neq \alpha^x$. The orbits of G are the sets of vertices of the (weakly) connected components of this

graph. In computing the orbits, one starts with the partition of the vertex set into subsets of size 1. Edges are then calculated one by one, and at each step two parts of the partition are merged into a single part if they are joined by the edge which has been generated. The final partition gives the partition of Ω into orbits.

For later purposes we note that, with very little extra computation, it is possible, while computing the orbits, to generate for each orbit a representative γ and a subset $U \subseteq G$ such that each element in the orbit has a unique representation in the form γ^u $(u \in U)$.

(B) Computing Blocks

In order to check for primitivity and to calculate blocks, we proceed as follows. Let α, β be distinct points in Ω. Consider the digraph $\mathcal{G}$ with vertex set Ω and with edges consisting of pairs $(\alpha, \beta)^x$ $(x \in G)$. Note that this edge set is the smallest set of pairs which contains (α, β) and is closed under the action of the elements of W (since G is finite, every element in G is a product of elements from W). The calculation of the (weakly) connected components of $\mathcal{G}$ is similar to the corresponding calculation for orbits. The set of vertices in the connected component of $\mathcal{G}$ which contains the vertex α is the smallest block for G containing α and β (Exercise 3.6.1). In particular, if this calculation is carried out for fixed α and all $\beta \neq \alpha$, we shall either determine that G is primitive (the graph is connected for each β), or else find the minimal nontrivial blocks containing α.

(C) Bases and Strong Generating Sets

Many computations dealing with permutations groups use bases and a special type of generating set called a *strong generating set.* We shall first describe what a strong generating set is, and how a base and strong generating set can be used to solve problems such as the Order Problem and the Membership Problem. Later we shall explain how they can be computed.

Recall that a base for G is a subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = 1$. For computational purposes we shall assume that the points of the base are ordered, say, $\delta_1, \delta_2, \ldots, \delta_d$. We then define a chain of subgroups of G:

$$G = G(0) \geq G(1) \geq \ldots \geq G(d) = 1$$

where $G(i) = G(i-1)_{\delta_i}$ for $i = 1, \ldots, d$. A *strong generating set* U for G with respect to this ordered basis is a subset of G such that $U \cap G(i)$ is a set of generators for $G(i)$ $(i = 0, 1, \ldots, d)$. In the present discussion we shall only be interested in a special form of strong generating set where $U = \cup_{i=1}^{d} U_i$ and U_i is a set of right coset representatives for $G(i)$ in $G(i-1)$ for $i = 1, 2, \ldots d-1$. In addition to the sets U_i we shall assume that, for each i, we also know the orbit Δ_i of δ_i in $G(i-1)$ and the bijective correspondence $\Delta_i \rightarrow U_i$ given by $\alpha \mapsto u_i(\alpha)$ where $\alpha = \delta_i^{u_i(\alpha)}$. If we have this information then clearly the Order Problem is solved since $|G| = \prod_{i=1}^{d} |\Delta_i|$.

The Membership Problem is solved as follows. Let $x \in Sym(\Omega)$. We recursively define x_i by

$$x_0 := x \quad \text{and} \quad x_i := x_{i-1}u_i(\delta_i^{x_{i-1}})^{-1} \in G(i) \quad \text{for } i = 1, 2, \ldots$$

as long as $i \leq d$ and $\delta_i^{x_{i-1}} \in \Delta_i$. This process is called *stripping*. If the stripping process stops before i reaches d, then clearly $x \notin G$. On the other hand, if i reaches d then

$$x = u_d(\delta_d^{x_{d-1}})^{-1}u_{d-1}(\delta_{d-1}^{x_{d-2}})^{-1} \ldots u_1(\delta_1^{x_0})^{-1} \in G.$$

Thus the Membership Problem is solved, and if $x \in G$ we have expressed x as a product of elements from our strong generating set U. We also note that if the stripping process stops at index $i < d$ (and so $x \notin G$), we obtain an element x_i which fixes $\delta_1, \ldots, \delta_i$ and is contained in the group $< G, x >$.

(D) Schreier Generating Sets

The construction of a generating set U of the kind described above is based on a theorem due to O. Schreier.

Theorem 3.6A. *Let H be a subgroup of a finite group G and let T be a set of right coset representatives for H in G. Assume that $1 \in T$ and define the mapping $\psi : G \to T$ by $Hx = H\psi(x)$ (so ψ chooses the correct coset representative of Hx from T). If W is a set of generators of G, then*

$$V := \{tw\psi(tw)^{-1} \mid x \in W, t \in T\}$$

is a set of generators for H.

PROOF. Since $Htw = H\psi(tw)$ by the definition of ψ, we have $V \subseteq H$. Thus it is enough to show that each $y \in H$ can be written as a product of elements from V. Since W generates G, and G is finite, we can write $y = w_1w_2 \cdots w_m$ for some $w_i \in W$ and some $m \geq 0$. Then, taking $t_0 = 1 \in T$, we have

$$y = t_0w_1w_2 \cdots w_m = (t_0w_1t_1^{-1})(t_1w_2t_2^{-1}) \cdots (t_{m-1}w_mt_m^{-1})t_m$$

where $t_i := \psi(t_{i-1}w_i)$ for $i = 1, 2, \ldots, m$. Each factor $t_{i-1}w_it_i^{-1} \in V$, and $t_m \in H \cap T$ since $V \subseteq H$ and $y \in H$. Hence $t_m = t_0 = 1$, and so y has been expressed as a product of elements from V as required. □

(E) Constructing a Base and Strong Generating Set for G

The process proceeds recursively. At a general step we have computed a partial base $\delta_1, \ldots, \delta_{i-1}$, and for the corresponding subgroups $G(0) \geq G(1) \ldots \geq G(i-1)$ we have the orbits $\Delta_1, \ldots, \Delta_{i-1}$ and the sets of right coset representatives $U_1, \ldots, U_{i-1}$ with bijective correspondences between Δ_j and U_j $(j = 1, \ldots, i-1)$. We shall also have a generating set W_{i-1} for $G(i-1)$. If $W_{i-1} = \emptyset$ then we are finished, so assume that $W_{i-1} \neq \emptyset$; we

want to calculate δ_i, Δ_i, U_i and W_i. Choose δ_i to lie in the support of some element of W_{i-1}, and use the technique for computing orbits described in (A) to calculate the orbit Δ_i of δ_i under $G(i-1)$, a set U_i of right coset representatives for $G(i) := G(i-1)_{\delta_i}$, and the bijective correspondence between Δ_i and U_i described there. Now use W_{i-1} and U_i and the Schreier Theorem to compute a set W_i of generators for $G(i)$. In practice, this is the trickiest part, since if care is not taken the sizes of the generating sets grow very quickly (Schreier's Theorem gives a set of $|W_{i-1}|\,|U_i|$ generators). This problem is alleviated by calculating the Schreier generators one by one, and discarding those which already lie in the group generated by the previously calculated generators. This requires solution of the membership problem for this smaller group and is done (recursively!) by working with a base and strong generating set for the subgroup of $G(i)$ which is generated up to that point.

Exercises

3.6.1 Prove that the algorithm in (B) does indeed produce the smallest blocks containing the point α.

3.6.2 Suppose that you are given two transitive permutation representations of a finite group G, specified by giving the images of a set of generators of G. Describe an algorithm to determine whether the two representations are equivalent.

3.6.3 Carry out the construction described in (E) for the group $G = \langle(12), (123), (14)(25)(36)\rangle$ and hence find its order.

3.6.4 Given a strong generating set U for G of the form described in (E), explain how to generate random elements of G with a uniform distribution. (Compare with Exercise 1.2.11).

3.6.5 (Computing coset representatives for G in $Sym(\Omega)$)

(i) If $\Delta \subseteq \Gamma$, describe an explicit set V of right coset representatives for $Sym(\Delta) \times Sym(\Gamma \setminus \Delta)$ in $Sym(\Gamma)$.

(ii) In general, suppose that $G \leq Sym(\Omega)$ and that we have a base $\{\delta_1, \ldots, \delta_d\}$ and strong generating set for G. Assume the notation of (E), and define partitions $\Pi_0, \ldots, \Pi_d$ of Ω as follows, starting with $\Pi_0 := \{\Omega\}$. For $i = 1, 2, \ldots, d-1$:

(a) show that each part of Π_{i-1} is $G(i-1)$-invariant, so there is one part, say Γ_i, which contains Δ_i;

(b) define Π_i as the refinement of Π_{i-1} obtained by replacing the part Γ_i by the three parts: $\{\delta_i\}$, $\Delta_i \setminus \{\delta_i\}$ and $\Gamma_i \setminus \Delta_i$ (excluding empty subsets);

(c) use (i) to construct a set V_i of right coset representatives for $Sym(\Delta_i) \times Sym(\Gamma_i \setminus \Delta_i)$ in $Sym(\Gamma_i)$.

(iii) With the notation of (ii), show that G has a set of right coset representatives in $Sym(\Omega)$ of the form $V^* V_d V_{d-1} \ldots V_1$ where $V^* := \prod_{\Gamma \in \Pi_d} Sym(\Gamma)$.

3.6.6 (Selecting conjugacy classes of S_n at random) Consider the following process of choosing a list $(n_1, n_2, \ldots)$ of positive integers whose sum is n: first n_1 is chosen so that it is equally likely to be any integer in the interval $[1, n]$; then n_2 is chosen so that it is equally likely to be any integer in the interval $[1, n - n_1]$; and, in general, n_i is chosen so that it is equally likely to be any integer in the interval $[1, n - n_1 - \cdots - n_{i-1}]$. This process is continued until $n_1 + n_2 + \cdots + n_k = n$, and we then stop. We associate the final list $(n_1, n_2, \ldots, n_k)$ with the conjugacy class of S_n consisting of elements of S_n whose disjoint cycles have lengths $n_1, n_2, \ldots, n_k$. Prove that the probability of obtaining a specific conjugacy class is proportional to the size of the class.

3.7 Notes

- Sect. 3.2: An early use of graphs to analyze permutation groups appears in Higman (1964) and Sims (1967). We have used the exposition of Neumann (1977) in this section.
- Theorem 3.2A: See Higman (1967).
- Exercise 3.2.12: The distinction between primitive and strongly primitive groups (which applies only to infinite groups) was introduced in Wielandt (1960b).
- Theorem 3.2B and Lemma 3.2B: These are classical; the proofs follow Neumann (1977).
- Exercises 3.2.19–20: See Weiss (1935).
- Theorem 3.2C: See Wielandt (1964).
- Theorem 3.2D: See Praeger (1977) and (1979).
- Exercise 3.2.29: See Neumann (1977).
- Sect. 3.3: The concept of minimal degree is classical, but the explicit idea of a base seems to have introduced in Sims (1970). Most results in this section are classical and were known to Jordan.
- Theorem 3.3B: See Bochert (1889).
- Lemma 3.3A: See Neumann (1954) and Tomkinson (1987).
- Theorem 3.3C: See Birch et al. (1976) and Neumann (1976).
- Theorems 3.3D and 3.3E: Also theorems of Jordan. Since "many" permutations in S_n have a power which is a prime cycle or has small support, these theorems help to explain why "most" elements do not lie in proper primitive subgroups. This idea is exploited in Dixon (1969), Bovey and Williamson (1978), Bovey (1980) and Babai (1989). See Liebeck and Saxl (1985a) for a far-reaching generalization of Theorem 3.3E.
- Sect. 3.4: The theorem of Frobenius (1902) showing that a finite Frobenius group has a regular normal subgroup was one of the earliest successes of the theory of linear representations, and still no more elementary proof available. Special cases of the result were known before then (see Burn-

side (1911) §134), and "elementary" cases have been found since then (see the remarks before Theorem 3.4A). The structure of the stabilizer of a finite Frobenius group was determined by Zassenhaus (1936) in the context of finite groups which act fixed point free. Finally, Thompson (1959) showed that every finite group with a fixed point free automorphism of prime order is nilpotent, and so showed that the Frobenius kernel is nilpotent. These results are developed in full in Passman (1968) (see also Huppert (1967) V §7–§8).

- Exercise 3.4.6–7: See Janko (1964) and Herstein (1958).
- Theorem 3.4A: See Burnside (1911) §134.
- Theorem 3.4B: Part (i) is due to Jordan (1872). For (ii) see Tits (1952).
- Examples 3.4.2–4: See Collins (1990).
- Sect. 3.5: These are classical results. We have used the method of Schur (1933) ("S-rings") as developed by Wielandt (1964) in this section.
- Lemmas 3.5A: and 3.5B See Wielandt (1964) and (1969).
- Theorem 3.5A: This is a generalization by Wielandt (1935) of earlier theorems of Burnside and Schur. See also Wielandt (1964).
- Exercise 3.5.9: Lidl and Muller (1993) gives a survey of results on permutation polynomials.
- Theorem 3.5B: This is the original theorem of W. Burnside. Its many proofs include: a proof using representation theory (see Burnside (1911) §251 and many books dealing with representation theory), a proof using module theory (see Wielandt (1969) Chap. 3 or Passman (1968) Theorem 7.3), and a proof using finite geometries (see Dress et al. (1992)). We have chosen a proof due to Schur (1908) since it is quite direct. For related results, see Bercov (1965), Neumann (1972) and (1974), Klemm (1975) and (1977) and Levingston (1978).
- Exercise 3.5.12: See Itô (1992).
- Sect. 3.6: Computational methods in permutation groups have developed over the last 25–30 years beginning with early work of C. C. Sims who introduced the concept of base and strong generating set around 1970. Part of the discussion in this section is based on an unpublished report by Atkinson (1989). There is now a considerable literature on this topic, of which the following is a random sample: Bannai and Iwasaki (1974), Blaha (1992), Butler and Cannon (1982), Ivanov et al. (1983), Jerrum (1986), Knuth (1991), Leon (1980) and (1984),Luks (1987), Neumann (1987), Sims (1970) and (1978). Hoffmann (1982) contains an analysis of some of the theoretical problems of such computations, and conference proceedings of Atkinson (1984) and Finkelstein and Kantor (1993) include several papers of interest in this area. The book of Sims (1994) is of related interest.
- Exercise 3.6.5: See Dixon and Majeed (1988).

4

The Structure of a Primitive Group

4.1 Introduction

In this chapter our focus changes from the combinatorial and ring theoretic representations of permutation groups considered in the last chapter to more direct group theoretic analysis of the groups involved. The point stabilizers of a primitive group form a conjugacy class of maximal subgroups, so classification of primitive groups is closely related to a study of maximal subgroups. Although some of the results in this chapter are valid for infinite groups, the central theorems will apply only to finite groups.

It turns out that the key to analyzing finite primitive groups is to study the socle, which is the subgroup generated by the minimal normal subgroups (see Sect. 4.3). In general, the socle of a finite group has fairly transparent structure: it is a nontrivial direct product of simple groups. When G is a finite primitive group, these simple groups are all isomorphic, and we can describe in some detail how the socle is embedded into G. The O'Nan–Scott Theorem (Theorem 4.1A) summarizes these results. Combined with the classification of finite simple groups, this theorem has proved to be a very powerful tool in answering some long-standing questions about finite permutation groups (see Sect. 4.8).

In studying this chapter there is a danger of being overcome by the technicalities necessary even to give precise statements of the main results. It may be useful, therefore, to keep in mind the following summary of the principal theorem (see also Sect. 4.8).

Theorem 4.1A (O'Nan–Scott Theorem). *Let G be a finite primitive group of degree n, and let H be the socle of G. Then either*

(a) *H is a regular elementary abelian p-group for some prime p, $n = p^m := |H|$, and G is isomorphic to a subgroup of the affine group $AGL_m(p)$; or*

(b) *H is isomorphic to a direct power T^m of a nonabelian simple group T and one of the following holds:*

  (i) *$m = 1$ and G is isomorphic to a subgroup of* $\mathrm{Aut}(T)$*;*

(ii) *$m \geq 2$ and G is a group of "diagonal type" with $n = |T|^{m-1}$;*
(iii) *$m \geq 2$ and for some proper divisor d of m and some primitive group U with a socle isomorphic to T^d, G is isomorphic to a subgroup of the wreath product U wr $Sym(m/d)$ with the "product action", and $n = \ell^{m/d}$ where ℓ is the degree of U;*
(iv) *$m \geq 6$, H is regular, and $n = |T|^m$.*

Groups of "diagonal type" and wreath products with the "product action" are discussed in Sect. 4.5. More detailed statements and proofs of the various parts of Theorem 4.1A are found in Sect. 4.6 and 4.7 (the nonregular and regular socles, respectively). The earlier sections of this chapter give a careful description of the centralizer and normalizer of a transitive subgroup in the symmetric group, the basic facts about socles, and a little about subnormal subgroups and composition factors.

In the special case of a 2-transitive group, Theorem 4.1A has a much simpler form.

Theorem 4.1B. *The socle of a finite 2-transitive group is either a regular elementary abelian p-group, or a nonregular nonabelian simple group.*

This result was originally proved by W. Burnside (see Burnside (1911) §154, Th. XIII), and was an early forerunner of the O'Nan–Scott Theorem. In Sect. 4.8 we will see that a primitive group coming under parts (b)(ii),(b)(iii) or (b)(iv) of Theorem 4.1A must have rank at least 3, thus proving Theorem 4.1B.

4.2 Centralizers and Normalizers in the Symmetric Group

Suppose that G is a transitive subgroup of $Sym(\Omega)$ (we are not restricting Ω to be finite). In this section we shall look at the centralizer and normalizer of G in $Sym(\Omega)$. The results are basic, and will be used repeatedly in the subsequent analysis of primitive groups. We begin with two exercises which illustrate some of the important ideas.

Exercises

4.2.1 Let C be the centralizer in $Sym(\Omega)$ of the subgroup $G \leq Sym(\Omega)$. Show that for each point $\alpha \in \Omega$ the orbit α^C is contained in $\mathrm{fix}(G_\alpha)$.

4.2.2 Let G be a nontrivial group and consider two ways in which G can act on itself:
  (i) (Right multiplication) $\rho : G \to Sym(G)$ defined by $a^{\rho(x)} := ax$; and
  (ii) (Left multiplication) $\lambda : G \to Sym(G)$ defined by $a^{\lambda(x)} := x^{-1}a$ (see Example 1.3.4 and Exercise 1.3.2).

Show that the images of ρ and λ centralize each other, and that for some t of order 2 in $Sym(G)$ we have $t^{-1}\rho(G)t = \lambda(G)$.

We can generalize the last exercise as follows. Fix a subgroup H of the group G. Then G acts by right multiplication on the set Γ_H of right cosets of H. Earlier we denoted this permutation representation by ρ_H (see Example 1.3.4), but here we shall simply denote it by ρ. If we restrict our attention to the normalizer $K := N_G(H)$, then there is a second action λ of K on Γ_H given by left multiplication; namely, $(Ha)^{\lambda(x)} := x^{-1}(Ha) = Hx^{-1}a$. The lemma below examines the relationship between the images $\rho(G)$ and $\lambda(K)$.

We say that a group G acts *semiregularly* on a set Ω if G acts on Ω in such a way that the identity is the only element with any fixed points; in other words, $G_\alpha = 1$ for all $\alpha \in \Omega$. In particular, a group is regular if and only if it is both semiregular and transitive.

Lemma 4.2A. *Let G be a group with a subgroup H, and put $K := N_G(H)$. Let Γ_H denote the set of right cosets of H in G, and let ρ and λ denote the right and left actions of G and K, respectively, on Γ_H as defined above. Then:*

(i) $\ker\lambda = H$ *and $\lambda(K)$ is semiregular;*
(ii) *The centralizer C of $\rho(G)$ in $Sym(\Gamma_H)$ equals $\lambda(K)$;*
(iii) *$H \in \Gamma_H$ has the same orbit under $\lambda(K)$ as under $\rho(K)$;*
(iv) *If $\lambda(K)$ is transitive, then $K = G$, and $\lambda(G)$ and $\rho(G)$ are conjugate in $Sym(\Gamma_H)$.*

PROOF. (i) Clearly $x^{-1}Ha = Ha$ for all $a \in G \iff x \in H \iff x^{-1}Ha = Ha$ for some $a \in G$. Thus $\ker\lambda = H$, and the point stabilizer of each point $Ha \in \Gamma_H$ under the action λ is H.

(ii) First, note that if $x \in G$ and $y \in K$, then for each $a \in G$:

$$(Ha)^{\rho(x)\lambda(y)} = Hy^{-1}ax = (Ha)^{\lambda(y)\rho(x)}$$

and so $\rho(x)\lambda(y) = \lambda(y)\rho(x)$. Thus $\lambda(K) \le C$.

Conversely, suppose that $z \in C$ and that $H^z = Hc$, say. Then for each $a \in G$:

$$(Ha)^z = H^{\rho(a)z} = H^{z\rho(a)} = Hca.$$

In particular, for each $a \in H$, we have $Hc = (Ha)^z = Hca$. Thus $c \in N_G(H) = K$, and $z = \lambda(c^{-1})$. This shows that $C \le \lambda(K)$ and completes the proof of (ii).

(iii) In both cases the orbit of H is the set of right cosets of H in K.

(iv) If $\lambda(K)$ is transitive, then (iii) shows that each coset Hx ($x \in G$) has the form $H^{\rho(y)} = Hy$ for some $y \in K$. Hence $G = K = N_G(H)$ and so $H \lhd G$. Thus we can define a permutation $t \in Sym(\Gamma_H)$ by $(Ha)^t := Ha^{-1}$; the point is that when $H \lhd G$ this mapping is well-defined. Now verify that $t^{-1}\lambda(x)t = \rho(x)$ for all $x \in G$. □

Using this lemma we can analyze the centralizer of a transitive group.

Theorem 4.2A. *Let G be a transitive subgroup of $Sym(\Omega)$, and α a point in Ω. Let C be the centralizer of G in $Sym(\Omega)$. Then:*

(i) *C is semiregular, and $C \cong N_G(G_\alpha)/G_\alpha$ (so $|C| = |\text{fix}(G_\alpha)|$ by Exercise 1.6.3);*
(ii) *C is transitive if and only if G is regular;*
(iii) *if C is transitive, then it is conjugate to G in $Sym(\Omega)$ and hence C is regular;*
(iv) *$C = 1$ if and only if G_α is self-normalizing in G (that is, $N_G(G_\alpha) = G_\alpha$);*
(v) *if G is abelian, then $C = G$;*
(vi) *if G is primitive and nonabelian, then $C = 1$.*

Proof. We apply the preceding lemma with $H = G_\alpha$. Since G and $\rho(G)$ are then permutation isomorphic, the lemma shows that C is permutation isomorphic to $\lambda(K)$ where $K = N_G(G_\alpha)$. Thus (i) follows from Lemma 4.2A (i), and (iv) follows from (i).

Using Lemma 4.2A (iii) and (iv) we now observe that C is transitive if and only if $\rho(K)$ is transitive, and that in the latter case C is conjugate to G in $Sym(\Omega)$. Since $\rho(K)$ is permutation isomorphic to K, and $K \geq G_\alpha$, this shows that C is transitive if and only if $K = G$. But $K = G$ holds exactly when $G_\alpha \triangleleft G$, and this is equivalent to $G_\alpha = 1$ and G being regular. Hence (ii) and (iii) follow.

If G is abelian, then $C \geq G$, and so (iii) shows that $C = G$; this proves (v). Finally, in the case that G is primitive, G_α is a maximal subgroup of G. Hence, if G is also nonabelian, then G_α must be its own normalizer in G. Thus (vi) follows from (iv). □

Exercises

4.2.3 Find the centralizer of $G = \langle (123456), (26)(35) \rangle$ in S_6.

4.2.4 Let C be the centralizer of an intransitive group G in $Sym(\Omega)$. Show that the orbits of G on Ω are equivalence classes for a C-congruence. Moreover, if Δ and Γ are G-orbits, then there exists $c \in C$ such that $\Delta^c = \Gamma$ if and only if the actions of G on Δ and Γ are equivalent. In particular, the union of all G-orbits of a fixed size is a C-invariant subset of Ω.

4.2.5 (Continuation) Let Σ be the set of orbits of G and suppose that the action of G on each of its orbits is equivalent to its action on a set Δ. Show that $C \cong C_0 \ wr_\Gamma \ Sym(\Gamma)$ where C_0 is the centralizer in $Sym(\Delta)$ of the subgroup G^Δ.

4.2.6 Let $T \subseteq Sym(\Omega)$ and let C be the centralizer of T. If $\alpha \in \Omega$, show that $\langle T \rangle$ is regular if and only if, for each $t \in T$ there exists $c \in C$ with $\alpha^t = \alpha^c$.

4.2.7 Show that the centralizer in $Sym(\Omega)$ of a semiregular subgroup of $Sym(\Omega)$ is transitive.

4.2.8 Suppose that H is a nontrivial and nonregular normal subgroup of a primitive group G. Show that each point stabilizer of H is its own normalizer in G, and that H has a trivial centralizer in G.

We shall now consider the normalizers of transitive groups. Let G be a transitive subgroup of $Sym(\Omega)$. Then the normalizer N of G in $Sym(\Omega)$ acts naturally on the set G by conjugation; this gives a homomorphism

$$\Psi : N \to \mathrm{Aut}(G) \quad \text{where} \quad \Psi(x) : u \mapsto x^{-1}ux.$$

Since $\ker \Psi$ is the centralizer of G in $Sym(\Omega)$, the previous theorem shows that Ψ is injective exactly when $N_G(G_\alpha) = G_\alpha$ for each $\alpha \in \Omega$. The following characterization of the automorphisms of G which lie in $\mathrm{Im}\,\Psi$ will be useful in the classification theorems developed later in this chapter.

Theorem 4.2B. *Let G be a transitive subgroup of $Sym(\Omega)$ and let $\alpha \in \Omega$. If Ψ is the homomorphism defined above, and $\sigma \in \mathrm{Aut}(G)$, then*

$$\sigma \in \mathrm{Im}\,\Psi \iff (G_\alpha)^\sigma \quad \textit{is a point stabilizer for} \quad G.$$

PROOF. Let $\sigma \in \mathrm{Im}\,\Psi$, so $\sigma = \Psi(x)$ for some $x \in N$. Then $(G_\alpha)^\sigma = x^{-1}G_\alpha x = G_\beta$ where $\beta = \alpha^x$. Conversely, suppose that $(G_\alpha)^\sigma = G_\beta$ for some $\beta \in \Omega$. Then the two transitive permutation representations of G into $Sym(\Omega)$ given by $x \mapsto x$ and $x \mapsto x^\sigma$ are equivalent because G_β is a point stabilizer for each of them. This means that for some $t \in Sym(\Omega)$ we have $xt = tx^\sigma$ for all $x \in G$. Clearly $t \in N$. Hence $\sigma = \Psi(t) \in \mathrm{Im}\,\Psi$ as required. □

In the special case when G is regular, N is the holomorph of G (see Exercise 2.5.6). We then have the following result.

Corollary 4.2B. *If G is regular, then $\mathrm{Im}\,\Psi = \mathrm{Aut}(G)$. In this case $N_\alpha \cong \mathrm{Aut}(G)$, and N is isomorphic to the semidirect product $G \rtimes \mathrm{Aut}(G)$ with the natural action of $\mathrm{Aut}(G)$ on G.*

PROOF. Since G is regular, therefore $G_\alpha = 1$, and so $\mathrm{Im}\,\Psi = \mathrm{Aut}(G)$ by the theorem. The centralizer C of G in $Sym(\Omega)$ is regular and isomorphic to G by Theorem 4.2A, and therefore $N = CN_\alpha$ with $C \triangleleft N$ and $C \cap N_\alpha = 1$. Hence $\mathrm{Aut}(G) = \mathrm{Im}\,\Psi \cong N/\ker\Psi = N/C \cong N_\alpha$. Finally, because G is regular and normal in N, therefore $G \cap N_\alpha = 1$ and $N = GN_\alpha \cong G \rtimes \mathrm{Aut}(G)$. □

Exercises

4.2.9 In the context of Theorem 4.2B give an example of a transitive group G for which $\mathrm{Im}\,\Psi$ is not all of $\mathrm{Aut}(G)$.

4.2.10 Calculate the normalizer of a Sylow p-subgroup in S_{p^2}.

4.2.11 Let $n \geq 1$ and let $\Omega = \mathbb{Z}/n\mathbb{Z}$ (the ring of integers modulo n). Let H be the set of all mappings of Ω into itself of the form: $\xi \mapsto r\xi + s$ where $r, s \in \mathbb{Z}/n\mathbb{Z}$ and the integers in the congruence class r are relatively prime to n. Show that H is a subgroup of $Sym(\Omega)$, and that H is the holomorph of a cyclic group of order n.

4.2.12 (Continuation) Enumerate all the transitive subgroups of H.

4.2.13 Show that the holomorph of a group G is primitive if and only if G has no characteristic subgroups apart from 1 and G.

4.2.14 If the holomorph of a group G is 2-transitive, show that all nontrivial elements of G have the same order. In particular, if G is finite, show that G is an elementary abelian p-group for some prime p (each nontrivial element has order p). (The case for infinite groups is more complicated since it is known that there exist infinite non-abelian simple groups in which every pair of nontrivial elements are conjugate. See Higman et al. (1949).)

4.2.15 Show that the affine group $AGL_d(p)$ is the holomorph of the elementary abelian p-group of order p^d.

4.2.16 Give an example of two nonisomorphic finite groups which have isomorphic holomorphs.

4.2.17 Let G be a finite permutation group containing a regular normal subgroup K. If $H \leq G$ and $\Delta := \mathrm{fix}(H) \neq \emptyset$, show that $(C_G(H) \cap K)^{\Delta}$ is regular in $Sym(\Delta)$.

4.3 The Socle

The major theme of this chapter is the analysis of a finite primitive group in terms of its socle. This section defines the socle and describes the form that it can take in a finite primitive group.

A *minimal normal subgroup* of a nontrivial group G is a normal subgroup $K \neq 1$ of G which does not contain properly any other nontrivial normal subgroup of G. For example, a simple group has itself as its only minimal normal subgroup, while an infinite cyclic group has no minimal normal subgroup. The *socle* of a group G is the subgroup generated by the set of all minimal normal subgroups of G; it is denoted by $\mathrm{soc}(G)$. By the usual convention, $\mathrm{soc}(G) = 1$ if G has no minimal normal subgroups.

Since the set of all minimal normal subgroups of G is mapped into itself by every automorphism of G, the socle $\mathrm{soc}(G)$ is a characteristic subgroup of G. Every nontrivial finite group has at least one minimal normal subgroup so has a nontrivial socle.

Exercises

4.3.1 Find the socle of S_4.

4.3.2 Let G be the multiplicative group consisting of all complex numbers z which are roots of unity (so $z^n = 1$ for some $n > 0$ depending on z). Find $\mathrm{soc}(G)$.

4.3.3 If G is a finite p-group, show that $\mathrm{soc}(G)$ is contained in the centre $Z(G)$.

4.3.4 If G is a direct product of a finite number of simple groups, show that $G = \mathrm{soc}(G)$. Is this still true for a direct product of an infinite number of simple groups?

4.3.5 If F is the free group on two generators, show that $\mathrm{soc}(F) = 1$.

We now turn to our analysis of the socle for a finite group. Although the socle of a group is defined simply as the subgroup generated by the set of minimal normal subgroups, the following theorem shows that it is actually a direct product of some or all of these normal subgroups.

Theorem 4.3A. *Let G be a nontrivial finite group.*

(i) *If K is a minimal normal subgroup of G, and L is any normal subgroup of G, then either $K \leq L$ or $\langle K, L\rangle = K \times L$.*

(ii) *There exist minimal normal subgroups $K_1, \ldots, K_m$ of G such that* $\mathrm{soc}(G) = K_1 \times \ldots \times K_m$.

(iii) *Every minimal normal subgroup K of G is a direct product $K = T_1 \times \cdots \times T_k$ where the T_i are simple normal subgroups of K which are conjugate under G.*

(iv) *If the subgroups K_i in (ii) are all nonabelian, then $K_1, \ldots, K_m$ are the only minimal normal subgroups of G. Similarly, if the T_i in (iii) are nonabelian, then these are the only minimal normal subgroups of K.*

PROOF. (i) Since $K \cap L \lhd G$ the minimality of K shows that either $K \leq L$ or $K \cap L = 1$. In the latter case $\langle K, L\rangle = KL = K \times L$ because both K and L are normal.

(ii) Because G is finite we can find a set $\mathcal{S} = \{K_1, \ldots, K_m\}$ of minimal normal subgroups of G which is maximal with respect to the property that the subgroup H generated by $\mathcal{S}$ is a direct product $K_1 \times \cdots \times K_m$. It remains to show that $H = \mathrm{soc}(G)$; this will follow if we show that H contains all minimal normal subgroups of G. Let K be a minimal normal subgroup of G. Then (i) shows that either $K \leq H$ or $\langle K, H\rangle = K \times H$. The latter is impossible by the choice of $\mathcal{S}$. Hence H contains every minimal normal subgroup of G as required.

(iii) Let T be a minimal normal subgroup of K. Then the conjugates $x^{-1}Tx$ of T under elements $x \in G$ are also minimal normal subgroups of K. Choose a set $\{T_1, \ldots, T_k\}$ of these conjugates which is maximal with respect to the property that $L := \langle T_1, \ldots, T_k\rangle$ is a direct product $T_1 \times \cdots \times T_k$. Then using an argument analogous to that in (ii) we see that L contains all of the conjugates of T under G, and so $L \lhd G$. Since $1 \neq L \leq K$ and K is a minimal normal subgroup of G of K, we conclude

that $K = L = T_1 \times \cdots \times T_k$. Finally, for each T_i, the normal subgroups of T_i are clearly normal in K, so the minimality of T_i shows that it must be a simple group.

(iv) Suppose that G has a minimal normal subgroup K which is distinct from the K_i ($i = 1, \ldots, m$). Then (i) shows that K centralizes each of the K_i and so $K \leq Z(\mathrm{soc}(G))$. However, if each K_i is nonabelian, then $Z(K_i) = 1$ by (iii). This implies that $Z(\mathrm{soc}(G)) = 1$ and so $K = 1$ contrary to the choice of K. □

Corollary 4.3A. *Every minimal normal subgroup of a finite group is either an elementary abelian p-group for some prime p, or its centre is equal to 1.*

PROOF. This follows at once from part (iii). □

We shall use the following technical lemma in applications of Theorem 4.3A.

Lemma 4.3A. *Let $T_1, \ldots, T_m$ be simple nonabelian groups. Suppose that H is a group with distinct normal subgroups $K_1, \ldots, K_m$ such that $H/K_i \cong T_i$ for each i and $\bigcap K_i = 1$. Then $H \cong T_1 \times \cdots \times T_m$.*

PROOF. Proceed by induction on m. The result is clear for $m = 1$, so suppose that $m > 1$. Put

$$K^* := \bigcap_{i=1}^{m-1} K_i, \quad H^* := H/K^* \text{ and } K_i^* := K_i \,/\, K^* \quad \text{for } i = 1, \ldots, m-1.$$

Since $H^*/K_i^* \cong H/K_i \cong T_i$, induction shows that $H^* \cong T_1 \times \cdots \times T_{m-1}$. In particular, it follows from Exercise 4.3.6 below that H^* has only $m - 1$ maximal normal subgroups, and so $H \ncong H^*$ by the hypothesis on H. Thus $K^* \neq 1$ but $K^* \cap K_m = 1$ by hypothesis. Since H/K_m is simple, K_m is a maximal normal subgroup of H, and so $H = K^*K_m = K^* \times K_m$. Since $K^* \cong H/K_m \cong T_m$ and $K_m \cong H/K^* = H^*$, therefore $H \cong T_1 \times \cdots \times T_m$ as required. □

Exercises

4.3.6 Suppose that $G = T_1 \times \cdots \times T_m$ is a direct product of a finite number of nonabelian simple groups T_i. Show that these are the only minimal normal subgroups of G, and that G has exactly m maximal normal subgroups, namely, the centralizers $C_G(T_i)$ ($i = 1, \ldots, m$).

4.3.7 (Continuation) What can you say if exactly one of the T_i's is an *abelian* simple group?

4.3.8 Show that there are exactly $(p^n - 1)/(p - 1)$ minimal normal subgroups in an elementary abelian p-group of order p^m. How many maximal normal subgroups does this group have?

4.3.9 Suppose that T is a nonabelian simple group. Show that for each integer $k \geq 1$, $\mathrm{Aut}(T^k) \cong \mathrm{Aut}(T)\ wr_\Gamma\ Sym(\Gamma)$ where $|\Gamma| = k$.

4.3.10 Determine the minimal normal subgroups of the group $AGL_d(p^m)$ and express each of them as a direct product of simple groups. Use this to show that the condition that T be nonabelian in the preceding exercise cannot be omitted.

4.3.11 Let G and H be nontrivial finite groups. Is it always true that the socle of the wreath product $W := G\ wr\ H$ is contained in the base group of W?

We now apply these general results on socles to the special case of a finite primitive group. As we know from Theorem 1.6A, every nontrivial normal subgroup of a primitive group is transitive. This imposes severe conditions on the minimal normal subgroups of a primitive group.

Theorem 4.3B. *If G is a finite primitive subgroup of $Sym(\Omega)$, and K is a minimal normal subgroup of G, then exactly one of the following holds:*

(i) *for some prime p and some integer d, K is a regular elementary abelian group of order p^d, and* $\mathrm{soc}(G) = K = C_G(K)$;

(ii) *K is a regular nonabelian group, $C_G(K)$ is a minimal normal subgroup of G which is permutation isomorphic to K, and* $\mathrm{soc}(G) = K \times C_G(G)$;

(iii) *K is nonabelian, $C_G(K) = 1$ and* $\mathrm{soc}(G) = K$.

Remark. Note that in case (iii) K may or may not be regular. In cases (i) and (iii) the socle is the unique minimal normal subgroup of G, and in case (ii) G has exactly two (isomorphic) minimal normal subgroups (see Theorem 4.3A (iv)). Affine groups give examples of case (i), and Theorem 4.7A shows that these (and their subgroups) are the only examples. An instance of case (ii) is given in Exercise 2.5.9, and any simple nonabelian primitive group gives an example of case (iii).

PROOF. Put $C := C_G(K)$. Since $C \triangleleft G$, either $C = 1$ or C is transitive. Since K is transitive, Theorem 4.2A shows that C is semiregular, and hence either $C = 1$ or C is regular; in the latter case C is the full centralizer of K in $Sym(\Omega)$, and so is permutation isomorphic to K. If C is regular, then it must be a minimal normal subgroup of G since any proper subgroup of C is intransitive. Theorem 4.3A (i) shows that every minimal normal subgroup of G distinct from K is contained in C. Thus in all cases we have $\mathrm{soc}(G) = KC$ which equals K or $K \times C$ depending on whether $C \leq K$ or not.

If $C = 1$, then we have case (iii); and, if $C = K$, then K is abelian and we have case (i) by the Corollary 4.3A. In the remaining case $\mathrm{soc}(G) = K \times C$ and we have case (ii). □

Corollary 4.3B. *If G is a finite primitive group, then $H := \mathrm{soc}(G)$ is a direct product of isomorphic simple groups. If N denotes the normalizer of H in the symmetric group, then H is a minimal normal subgroup of N. Moreover, if H is not regular, then it is the only minimal normal subgroup of N.*

PROOF. The first statement follows immediately in case (i), and follows from Theorem 4.3A in cases (ii) and (iii). Consider the second statement. Since $G \leq N$, we know that N is primitive, and $H \lhd N$. In cases (i) and (iii) $H = K$ is minimal normal in G and hence also minimal normal in N. In the case (ii) $C = C_G(K)$ is permutation isomorphic to K, and so $C = t^{-1}Kt$ for some $t \in Sym(\Omega)$. Then $t^{-1}Kt$ centralizes K, and so $t^{-1}Ct = t^{-2}Kt^2$ is contained in K because it centralizes $t^{-1}Kt = C$; thus comparing orders gives $t^{-1}Ct = K$. This shows that K and C are interchanged under conjugation by t. Since $H = K \times C$ in case (ii), we conclude that $t \in N$ and H is a minimal normal subgroup of N as asserted.

Finally, suppose that H is not regular, and apply the theorem to the primitive group N and its minimal normal subgroup H. Clearly, only case (iii) can apply, and so $H = \mathrm{soc}(N)$ is the unique minimal normal subgroup of N. □

Exercises

4.3.12 Show that each maximal primitive subgroup of S_n has a unique minimal normal subgroup.

4.3.13 Let H be the socle of a primitive subgroup of S_n, and let N denote the normalizer of H in S_n. If H is not regular, and G is a primitive subgroup of S_n such that $H \leq G \leq N$, show that $\mathrm{soc}(G) = H$. Give an example to show that this need not be true if H is regular.

4.3.14 Show that a permutation group of degree n with k orbits has at most $4(n-k)/3$ factors in its composition series. Moreover, this bound can be attained by a transitive group when n is a power of 4.

4.4 Subnormal Subgroups and Primitive Groups

The present section digresses from the main theme of this chapter to discuss the subnormal structure of the point stabilizers of a finite primitive group. This material will not be needed in the proof of the O'Nan–Scott Theorem, but it will be used in later chapters.

Recall that a subgroup H of a group G is *subnormal* in G if there is a finite chain of subgroups $H = H_0 \lhd H_1 \lhd \ldots \lhd H_d = G$ from H to G where each H_i is normal in H_{i+1} (but not necessarily in G). In a finite group, a subgroup is subnormal exactly when it appears in some composition series, so it is natural that subnormal subgroups arise in the study of the

composition factors of a finite group.. It is easily seen that a subnormal subgroup of G is also subnormal in every subgroup L of G in which it is contained. Clearly, every normal subgroup of G is subnormal, but, in general, a subnormal subgroup need not be normal (see Exercise 4.4.1).

Lemma 4.4A. *If G is a finite group, then* $\mathrm{soc}(G) \leq N_G(H)$ *for each subnormal subgroup H of G.*

PROOF. The result is certainly true if $G = H$, so we proceed by induction on $|G : H|$ and assume $H < G$. We have to show that each minimal normal subgroup K of G is contained in $N_G(H)$.

Since H is subnormal, there exists $L \triangleleft G$ with $H \leq L < G$. By Theorem 4.3A (i) we know that either $K \leq L$ or $\langle K, L \rangle = K \times L$. In the latter case $K \leq C_G(H) \leq N_G(H)$ and the result is true; so suppose $K \leq L$. Then there exists a minimal normal subgroup T of L with $T \leq K$. For each $x \in G, x^{-1}Tx$ is a minimal normal subgroup of $x^{-1}Lx = L$, so induction shows that $x^{-1}Tx \leq N_L(H) \leq N_G(H)$. Since K is a minimal normal subgroup of $G, K = \langle x^{-1}Tx \mid x \in G \rangle$, and so $K \leq N_G(H)$. This proves the lemma. □

The proof of the following lemma uses the elementary fact that if A and B are subgroups of any group G, then: $AB = BA \iff AB$ is a subgroup.

Lemma 4.4B. *Let H be a subgroup of finite index in a group G. If $Hx^{-1}Hx = x^{-1}HxH$ for all $x \in G$, then H is subnormal in G.*

PROOF. Proceed by induction on $|G : H|$. If $H \triangleleft G$, then the conclusion certainly holds, so suppose that $H \neq x^{-1}Hx$ for some $x \in G$ and put $K := Hx^{-1}Hx$. Now $|G : K| < |G : H|$, and the hypothesis on H clearly implies that $Ky^{-1}Ky = y^{-1}KyK$ for all $y \in G$. Therefore, by the induction hypothesis, K is subnormal in G. Moreover, $x \notin K$; otherwise, $1 \in Hx^{-1}H$, and that implies $x \in H$ contrary to the choice of x. Thus $|K : H| < |G : H|$, and so we can apply the inductive hypothesis to the pair K, H to conclude that H is subnormal in K. Since K is subnormal in G, this shows H is subnormal in G as asserted. □

Lemma 4.4C. *Let H be a subnormal subgroup of a finite group G, and consider the smallest normal subgroup $M := \langle x^{-1}Hx \mid x \in G \rangle$ of G containing H.*

(i) *Each composition factor of M is isomorphic to a composition factor of H, and each simple homomorphic image of M is isomorphic to a homomorphic image of H.*

(ii) *If K is a subnormal subgroup of G with no homomorphic image isomorphic to a composition factor of H, then $H \leq N_G(K)$.*

PROOF. (i) We proceed by induction on $|M : H|$. The result is trivial when $M = H$, so suppose that $M > H$. Then H is not normal in G, and we

have a chain $H = H_0 \lhd H_1 \lhd \ldots \lhd H_d = G$ of distinct subgroups of G with $d \geq 2$. Let k be the smallest index for which H_k is not contained in $N_G(H)$, and choose $x \in H_k \setminus N_G(H)$. Then H and $x^{-1}Hx$ are both normal subgroups of H_{k-1}, and so $L := Hx^{-1}Hx \lhd H_{k-1}$. Now $L \leq M$ and is a subnormal subgroup of G properly containing H. Since M is the smallest normal subgroup of G containing L, the inductive hypothesis shows that each composition factor of M is a composition factor of L, and each simple homomorphic image of M is a homomorphic image of L. On the other hand, $H_{k-1} \leq N_G(H)$ by the choice of k, so $H \lhd L$ and $L/H \cong x^{-1}Hx/(H \cap x^{-1}Hx)$. Thus, by the Jordan-Hölder Theorem, every composition factor of L is a composition factor of H. Similarly, if $N \lhd L$ and L/N is simple, then not both H and $x^{-1}Hx$ are contained in N; hence, either $H/(H \cap N)$ or $x^{-1}Hx/(x^{-1}Hx \cap N)$ is isomorphic to L/N. This proves (i).

(ii) It is enough to consider the case where $G = MK$ and show that in this case $K \lhd G$. Suppose that K is not normal in G. Then an argument similar to that given in (i) shows that for some $x \in G$, $L := Kx^{-1}Kx$ is subnormal in G and K is a proper normal subgroup of L. Then $L = L \cap MK = (L \cap M)K$, and so

$$x^{-1}Kx/(K \cap x^{-1}Kx) \cong L/K \cong (L \cap M)/(L \cap M \cap K). \tag{4.1}$$

Since L is subnormal in G, $L \cap M$ is subnormal in M, and so (4.1) shows that $x^{-1}Kx$ (and hence K) has a simple homomorphic image isomorphic to some composition factor of M. But then (i) shows that K has a simple homomorphic image isomorphic to some composition factor of H contrary to the hypothesis on K. Thus $K \lhd G$ and (ii) is proved. □

We now come to the main theorem of this section. If G is a finite primitive subgroup of $Sym(\Omega)$ and Γ is a nontrivial orbit of G_α then Theorem 3.2C shows that each composition factor of G_α is isomorphic to a section of the induced group G_α^Γ. Part (iii) of the theorem that follows extends this analysis to the stabilizer of two points $\alpha, \beta \in \Omega$. Let Λ be the orbital for G containing the pair (α, β), and let Λ^* be its paired orbital (see Section 3.2). Then $\Gamma = \Lambda(\alpha) = \beta^{G_\alpha}$ and $\Delta = \Lambda^*(\beta) = \alpha^{G_\beta}$ are $G_{\alpha\beta}$-invariant sets. Moreover, Γ and Δ have the same length.

Theorem 4.4A. *Let $G \leq Sym(\Omega)$ be a finite primitive group, and let $\alpha \in \Omega$.*

(i) *G_α contains no nontrivial subnormal subgroup of G.*

(ii) *If $\Sigma \subseteq \Omega$ is a union of orbits for G_α which contains one orbit from each pair of paired orbits (including the self-paired orbits), then G_α acts faithfully on Σ.*

(iii) *Let α and β be distinct points in Ω, and put $\Gamma := \beta^{G_\alpha}$ and $\Delta := \alpha^{G_\beta}$. Then each composition factor of $G_{\alpha\beta}$ is isomorphic to a composition factor of either $(G_{\alpha\beta})^\Gamma$ or $(G_{\alpha\beta})^\Delta$.*

PROOF. (i) Let H be a subnormal subgroup of G contained in G_α, and let K be any minimal normal subgroup of G. Then $G = KG_\alpha$ because G is primitive, and K normalizes H by Lemma 4.4A. Hence

$$M := \langle x^{-1}Hx \mid x \in G_\alpha \rangle = \langle y^{-1}Hy \mid y \in G \rangle \lhd G.$$

Since $M \leq G_\alpha$, $M = 1$ by the transitivity of G. Hence $H = 1$ as asserted.

(ii) Let $K := G_{(\Sigma)} \leq G_\alpha$ be the kernel of the action of G_α on Σ. First note that if Δ and Δ^* are paired orbitals for G, and $x \in G$ then:

$$\begin{aligned} \alpha^x \in \Delta(\alpha) &\iff (\alpha, \alpha^x) \in \Delta \\ &\iff (\alpha^{x^{-1}}, \alpha) \in \Delta \\ &\iff \alpha^{x^{-1}} \in \Delta^*(\alpha). \end{aligned}$$

Thus the hypothesis on Σ implies that, for each $x \in G$, at least one of α^x or $\alpha^{x^{-1}}$ lies in Σ. Since K fixes each point in Σ, this shows that for each $x \in G$ at least one of xKx^{-1} or $x^{-1}Kx$ is contained in G_α. However $K \lhd G_\alpha$, and $x^{-1}(KxKx^{-1})x = x^{-1}KxK$, so $Kx^{-1}Kx = x^{-1}KxK$ for all $x \in G$. Now Lemma 4.4B shows that K is subnormal in G, and so $K = 1$ by (i).

(iii) The result is trivial if G is regular, so suppose that G is not regular. Put $H := G_\alpha, K := G_\beta$ and $L := H \cap K = G_{\alpha\beta}$, and note that $L \neq 1$ and $G = \langle H, K \rangle$. Consider the condition:

(4.2) some simple homomorphic image of U is a composition factor of L^Γ or L^Δ

for subnormal subgroups U of L. If (4.2) holds for all nontrivial subnormal subgroups of L, then we can choose successive terms $L = L_0, L_1, \dots, L_d = 1$ in a composition series for L such that L_{i-1}/L_i is isomorphic to a composition factor of L^Γ or L^Δ for each i. The Jordan–Hölder Theorem then shows that every composition factor of L is isomorphic to a composition factor of L^Γ or L^Δ as required. On the other hand, suppose that (4.2) does not hold for some nontrivial subnormal subgroup of L, and choose $U \neq 1$ as a counterexample of maximal order; we shall show that this leads to a contradiction.

Since (4.2) fails to hold for U, U must lie in the kernel of the homomorphism $x \mapsto x^\Gamma$ of L onto L^Γ. Therefore $U \leq L_{(\Gamma)} = H_{(\Gamma)} \lhd H_{\{\Gamma\}} = H$, and so Lemma 4.4C (i) and the maximality of U show that $U \lhd H$. A similar argument shows that $U \lhd K$. Hence we conclude that $1 \neq U \lhd \langle H, K \rangle = G$ which is impossible because G is transitive and $U \leq H = G_\alpha$. Thus (4.2) holds for all nontrivial subnormal subgroups U of L, and the theorem is proved. □

Exercises

4.4.1 Find a subnormal subgroup of S_4 which is not normal.

4.4.2 Let H be a subnormal subgroup of a finite group G.
(i) If $\mathrm{soc}(G) \leq H$, show that $\mathrm{soc}(G) \leq \mathrm{soc}(H)$.
(ii) Show that $\mathrm{soc}(H)' \leq \mathrm{soc}(G)'$.
(iii) Give an example to show that $\mathrm{soc}(H)$ need not be contained in $\mathrm{soc}(G)$.

4.4.3 Show that the conclusion of Lemma 4.4C (i) need not be true if H is not subnormal.

4.4.4 With the notation of Theorem 4.4A give an example where $(G_\alpha)^\Gamma$ and $(G_\beta)^\Delta$ are not isomorphic.

4.4.5 Under the hypothesis of Theorem 4.4A show that $G_{\alpha\beta} = 1$ if $(G_\alpha)^\Gamma$ and $(G_\beta)^\Delta$ are both regular.

4.4.6 Under the hypothesis of Theorem 4.4A show that, if Γ (and hence Δ) has length d, then each prime p dividing $|G_{\alpha\beta}|$ satisfies $p < d$. (This gives an alternative solution to Exercise 3.2.25.)

4.4.7 If G is a finite primitive group whose point stabilizer G_α has an orbit Δ such that $(G_\alpha)^\Delta$ has prime order p, show that G is a Frobenius group of order pq^r for some prime $q \neq p$ and some $r \geq 1$.

4.4.8 If G is a finite primitive group with a regular normal subgroup, show that the point stabilizers act faithfully on each of their nontrivial orbits.

4.4.9 Suppose that a point stabilizer G_α of a finite primitive group G has a nontrivial centre $Z(G_\alpha)$. Show that G_β acts faithfully on α^{G_β} whenever $\beta \in \mathrm{supp}(Z(G_\alpha))$. [*Hint:* The kernel of the action of G_β on this orbit is normalized by $Z(G_\alpha)$.]

4.4.10 Let G be a finite primitive group with point stabilizer G_α. If there is an orbit Δ of G_α for which $(G_\alpha)^\Delta$ has order 4, show that G is a Frobenius group.

4.4.11 Show that, for any finite primitive group with a suborbit of length 3, the point stabilizers have order dividing $3 \cdot 2^4$.

4.4.12 If $G \leq \mathit{Sym}(\Omega)$ is an infinite primitive group with a finite nontrivial suborbit, show that all suborbits of G are finite and that Ω is countable.

4.4.13 Show that part (ii) of Theorem 4.4A fails for infinite groups. [*Hint:* Let $G := \mathrm{Aut}(\mathbb{Q}, \leq)$.] (Part (i) also fails, but this is more complicated.)

4.5 Constructions of Primitive Groups with Nonregular Socles

We continue to analyze the structure of a finite primitive group G in terms of its socle H. As we saw in Corollary 4.3B the socle of a finite primitive group is a direct product of isomorphic simple groups. When H is regular, G is contained in the holomorph of H, and we shall deal with this

situation later (see Sect. 4.7). In the present section we shall look at the case where H is not regular. Because G is primitive, we know that H is necessarily transitive, and in particular H cannot be abelian. This section deals with two general constructions of finite primitive permutation groups whose socles are nonregular.

Let $H = T_1 \times \cdots \times T_m$ be a direct product of m isomorphic copies of a finite nonabelian simple group T. Our objective is to embed H as a nonregular transitive subgroup in some symmetric group $Sym(\Omega)$ in such a way that the normalizer N of H in the symmetric group is primitive. Then N and certain subgroups G with $H \le G \le N$ will give examples of primitive groups which have H as a nonregular socle. We shall see in the next section that the constructions which we describe below give essentially all the primitive groups which have H as a nonregular socle when $m > 1$.

One of these constructions is already available directly from the product action of a wreath product (Sect. 2.7). Start with any transitive, nonregular representation of T; without loss in generality we may assume T is a transitive, nonregular subgroup of $Sym(\Delta)$, say. Let M be the normalizer of T in $Sym(\Delta)$, and put $\Gamma := \{1, \dots, m\}$. Then the wreath product $W := M \; wr_\Gamma \; Sym(\Gamma)$ acts faithfully on the set $\mathrm{Fun}(\Gamma, \Delta)$ of all functions of Γ into Δ with the product action. According to Theorem 2.7A, the image of this action is primitive exactly when M is primitive.

To simplify the notation we identify $\mathrm{Fun}(\Gamma, \Delta)$ with the Cartesian power Δ^m via $f \mapsto (f(1), \dots, f(m))$, and identify W with its image in $Sym(\Delta^m)$. We also identify H with the natural subgroup $T_1 \times \cdots \times T_m$ of the base group $M_1 \times \cdots \times M_m$ of W where the T_i are permutation isomorphic and $T \cong T_i \triangleleft M_i$ for each i. Note that all orbits of M_i have size $|\Delta|$ and are of the form

$$\{\delta_1\} \times \cdots \times \{\delta_{i-1}\} \times \Delta \times \{\delta_{i+1}\} \times \cdots \times \{\delta_m\}$$

and that these are also orbits for T_i. Moreover, the actions of M_i (and of T_i) on these different orbits are all equivalent. In general, if we fix $(\delta_1, \dots, \delta_m) \in \Delta^m$, then the stabilizer of this point in H has the form $R_1 \times \cdots \times R_m$ where, for each i, $R_i \le T_i$ is the stabilizer of δ_i in the action of T_i on Δ. Since H acts transitively on Δ^m, its point stabilizers are all conjugate, and so every point stabilizer of H has the form

$$u_1^{-1} R_1 u_1 \times \cdots \times u_m^{-1} R_m u_m \quad \text{with } u_i \in T_i \text{ for } i = 1, \dots, m.$$

Lemma 4.5A. *With the notation above, suppose that the normalizer N of H in $Sym(\Delta^m)$ is primitive. Then N is equal to the wreath product W.*

PROOF. Clearly $W \le N$, so it is enough to show that for each $x \in N$ we have $x \in W$. Let $\Sigma := \{T_1, \dots, T_m\}$. Since T is a nonabelian simple group, Theorem 4.3A (iv) shows that Σ is the set of all minimal normal subgroups of H, and hence W and N both act on Σ by conjugation. It is also clear that W induces the full symmetric group on Σ, and so for some

$y \in W$ we have $z := xy^{-1} \in N$ acting trivially on Σ. In particular, each T_i is normalized by z.

Since z normalizes H, conjugation by z must permute the point stabilizers of H amongst themselves. Since z acts trivially on Σ, this shows that conjugation by z must map each R_i onto a T_i-conjugate of itself. But the T_i-conjugates of R_i are the point stabilizers of T_i in its action on each of the orbits of T_i. Therefore Theorem 4.2B shows that the automorphism of T_i induced by conjugation under z is also induced by some element of M_i. Hence for some element $t \in M_1 \times \cdots \times M_m \leq W$, the element zt^{-1} centralizes $H = T_1 \times \cdots \times T_m$. Since N is primitive and H is not regular, Theorem 4.3B shows that $C_N(H) = 1$. Therefore $x = zy = ty \in W$ as required. □

The second general construction of a primitive group with nonregular socle also comes from the product action of a wreath product, but rather more indirectly. In this construction, take the simple nonabelian group T as a regular subgroup of $Sym(\Delta)$ and again put $\Gamma := \{1, \ldots, m\}$. Consider the wreath product $W := T \, wr_\Gamma \, S_m$ in its product action on Δ^m. Theorem 2.7A shows that W does not act primitively on Δ^m because T is regular, and indeed there is a fairly obvious W-congruence on Δ^m defined as follows. Let C be the centralizer of T in $Sym(\Delta)$; so C is also regular, and $C \cong T$ by Theorem 4.2A. Now C acts on Δ^m by $(\delta_1, \ldots, \delta_m)^c = (\delta_1^c, \ldots, \delta_m^c)$. This action commutes with the action of the base group of W since C centralizes T and commutes with the top group S_m since the same element of C acts on each component. Hence $(\delta_1, \ldots, \delta_m)^{cw} = (\delta_1, \ldots, \delta_m)^{wc}$ for all $c \in C, w \in W$ and $(\delta_1, \ldots, \delta_m) \in \Delta^m$. Thus the set Ω of all C-orbits in Δ^m is a set of blocks for W (see Exercise 4.5.1). We shall write $[\delta_1, \ldots, \delta_m] \in \Omega$ to denote the block containing $(\delta_1, \ldots, \delta_m)$. The corresponding action of the base group T^m on Ω is called the *diagonal action* of T^m.

Since T is regular on Δ, we can identify Δ with T, so that the action of T is right multiplication: $\delta^x = \delta x$ for all $x \in T$ and $\delta \in \Delta = T$. The action of the centralizer C is then left multiplication by the inverse: $\delta^c = c^{-1}\delta$. The C-orbit $[\delta_1, \ldots, \delta_m]$ consists of all points $(c^{-1}\delta_1, \ldots, c^{-1}\delta_m)$ for $c \in C$. These m-tuples are identified to a single point in Ω; the m-tuples $(\delta_1, \ldots, \delta_{m-1}, 1)$ may be taken as representatives, for example. With this identification, the base group T^m of W acts by right multiplication while the top group S_m permutes the components. It may be helpful to think of the construction of Ω "geometrically" as the analogue of the construction of a projective space from a vector space. The block $[\delta_1, \ldots, \delta_m]$ corresponds to the "1-dimensional subspace" through the "point" $(\delta_1, \ldots, \delta_m)$ (see Sect. 2.8).

Exercises

4.5.1 Suppose that G is a transitive subgroup of $Sym(\Gamma)$ and that $C \leq Sym(\Gamma)$ centralizes G. Show that the C-orbits form a set of blocks for G.

4.5.2 With the notation above, show that W acts faithfully on Ω.
4.5.3 Show that the point stabilizer of $[\delta, \dots, \delta]$ in W consists of all elements of W of the form $(u, \dots, u)s$ where $u \in T_\delta$ and $s \in S_m$.
4.5.4 Show that the diagonal action of W contains regular (but not normal) subgroups.

The product group $\mathrm{Aut}(T)^m$ acts on $\Delta^m = T^m$ with the element $(\tau_1, \dots, \tau_m)$ taking $(\delta_1, \dots, \delta_m)$ to $(\delta_1^{\tau_1}, \dots, \delta_m^{\tau_m})$. If this permutation induces an action on Ω then for any $c \in T$ we have $[(c^{-1}\delta_1)^{\tau_1}, \dots, (c^{-1}\delta_m)^{\tau_m}] = [\delta_1^{\tau_1}, \dots, \delta_m^{\tau_m}]$. This requires that all τ_i be equal. On the other hand, each automorphism $\tau \in \mathrm{Aut}(T)$ acts as a permutation of Ω by $[\delta_1, \dots, \delta_m]^\tau = [\delta_1^\tau, \dots, \delta_m^\tau]$. In fact, the action of the base group T^m already induces all of the inner automorphisms. Indeed, if $\tau \in \mathrm{Aut}(T)$ is conjugation by $x \in T$ then

$$\begin{aligned}
[\delta_1, \dots, \delta_m]^\tau &= [x^{-1}\delta_1 x, \dots, x^{-1}\delta_m x] \\
&= [\delta_1 x, \dots, \delta_m x] \\
&= [\delta_1, \dots, \delta_m]^x.
\end{aligned}$$

Note also that this action of $\mathrm{Aut}(T)$ commutes with the action of S_m. The next lemma shows that W can be extended by $\mathrm{Out}(T) = \mathrm{Aut}(T)/\mathrm{Inn}(T)$ to obtain the full normalizer of the diagonal action of T^m in $Sym(\Omega)$. We shall write S as the image of S_m and H as the image of the base group of the wreath product W in the action of W on Ω described above (Exercise 4.5.2 above shows that this action is faithful). In particular, $H = T_1 \times \cdots \times T_m$ where each T_i is isomorphic to T.

Lemma 4.5B (Diagonal type). *With the notation above, let N be the normalizer of H in $Sym(\Omega)$, so $W \cong HS \le N$. Then $N/HS \cong \mathrm{Out}(T)$.*

PROOF. Since T is a nonabelian simple group, the diagonal subgroup

$$D := \{(t, \dots, t) \mid t \in T\} \cong T$$

of T^m is self-normalizing in T^m. Therefore the point stabilizers of the (permutation isomorphic) group H (see Exercise 4.5.3) are also self-normalizing. In particular, H has a trivial centralizer in $Sym(\Omega)$ by Theorem 4.2A (iv). By Theorem 4.2B, the automorphisms of H induced by conjugation by elements of N are precisely those which permute the point stabilizers of H among themselves. Thus N is isomorphic to the group A of automorphisms of T^m which map D onto one of its conjugates in T^m. Since T is a nonabelian simple group, $\mathrm{Aut}(T^m) \cong \mathrm{Aut}(T)\ wr_\Gamma\ S_m$ where $\Gamma := \{1, \dots, m\}$ (Exercise 4.3.9). Using this representation of $\mathrm{Aut}(T^m)$, we see that if $\tau_1, \dots, \tau_m \in \mathrm{Aut}(T)$ and $s \in S_m$, then

$$\sigma := (\tau_1, \dots, \tau_m)s \in A \iff \text{for some } c \in T^m,\ D^\sigma = c^{-1}Dc.$$

Thus $\sigma \in A$ exactly when there are elements $c(1), \ldots, c(m) \in T$ such that for each $x \in T$ there exists $y \in T$, satisfying

$$x^{\tau_i} = c(i^s)^{-1} y c(i^s) \quad \text{for each } i.$$

But this implies that for all i and j, $\tau_i \tau_j^{-1} \in \mathrm{Inn}(T)$, and so all the τ_i lie in the same coset of $\mathrm{Inn}(T)$. Thus we can define a mapping $\Psi : A \to \mathrm{Aut}(T)/\mathrm{Inn}(T) = \mathrm{Out}(T)$ such that $\Psi(\sigma)$ is the coset of $\mathrm{Inn}(T)$ which contains all τ_i. It is easy to verify that Ψ is a homomorphism of A onto $\mathrm{Out}(T)$, and its kernel is $K := \mathrm{Inn}(T)\ wr_\Gamma\ S_m$. Moreover, K is isomorphic to $T\ wr_\Gamma\ S_m$ because $\mathrm{Inn}(T) \cong T$ for a simple nonabelian group T. Finally, N acting by conjugation on $H \cong T^m$ induces the subgroup A of automorphisms of T^m and in this correspondence HS induces K. Hence $N/HS \cong A/K \cong \mathrm{Out}(T)$ as asserted. □

We shall say that G is a group of *diagonal type* if G is a subgroup of the normalizer N of H in $Sym(\Omega)$ such that G contains the base group $H = T_1 \times \cdots \times T_m$ (so, by Lemma 4.5B, G is contained in an extension of the wreath product $T\ wr_\Gamma\ S_m$ by $\mathrm{Out}(T)$ where T is a finite nonabelian simple group). The analysis above shows that the point stabilizer G_α is isomorphic to a subgroup of $\mathrm{Aut}(T) \times S_m$ containing the group $\mathrm{Inn}(T) \cong T$. The groups $T_1, \ldots, T_m$ are the only minimal normal subgroups of H by Theorem 4.3A and $H \lhd G$, and so G acts by conjugation on the set $\{T_1, \ldots, T_m\}$. The following theorem characterizes those groups of diagonal type which are primitive.

Theorem 4.5A. *With the notation above, G is a primitive subgroup of $Sym(\Omega)$ exactly when either*
(i) *$m = 2$; or*
(ii) *$m \geq 3$, and the action of G by conjugation on the set $\{T_1, \ldots, T_m\}$ of minimal normal subgroups of H is primitive.*

In particular, the full normalizer N of the base group B is primitive for all $m \geq 2$.

PROOF. As before put $\Gamma := \{1, \ldots, m\}$, and let $V := \mathrm{Aut}(T)\ wr_\Gamma\ S_m$. The proof of Lemma 4.5B shows that N is isomorphic to

$$A := \{(\tau_1, \ldots, \tau_m)s \in V \mid s \in S_m \text{ and all } \tau_i \text{ lie in same } \mathrm{Inn}(T)\text{-coset}\}$$

and that under this isomorphism H maps onto

$$B := \{(\tau_1, \ldots, \tau_m)1 \in V \mid \text{ each } \tau_i \in \mathrm{Inn}(T)\}$$

and one of the point stabilizers of N maps onto

$$C := \{(\tau, \ldots, \tau)s \in V \mid \tau \in \mathrm{Aut}(T) \text{ and } s \in S_m\}.$$

Let L be the corresponding image of G. Then $L \cap C$ corresponds to a point stabilizer of G. Therefore Exercise 4.5.5 shows that G is primitive if and

only if there is no subgroup M of B such that

(4.3) $\quad B \cap C < M < B$ and M is normalized by $L \cap C$.

Finally, let

$$S := \{s \in S_m \mid (\tau_1, \ldots, \tau_m)s \in L\}.$$

It is easy to verify that S is permutation isomorphic to the image of the action of G on $\{T_1, \ldots, T_m\}$. Thus to prove the theorem it is enough to show that no subgroup M of B satisfies conditions (4.3) if and only if either (i) $m = 2$, or (ii) $m \geq 3$ and S is a primitive subgroup of S_m.

First, suppose that $m \geq 3$ and that S is not primitive. Then there is a nontrivial S-congruence, say $\equiv$, on Γ. Define

$$M := \{(\tau_1, \ldots, \tau_m)1 \in B \mid \tau_i = \tau_j \text{ whenever } i \equiv j\}.$$

Then it is straightforward to verify that M is a subgroup of B satisfying conditions (4.3). Therefore conditions (i) and (ii) are necessary.

Second, suppose that M is a subgroup which satisfies conditions (4.3). Consider the projections $\pi_i : M \to \mathrm{Inn}(T)$ defined by $(\tau_1, \ldots, \tau_m) \mapsto \tau_i$. Each π_i is a homomorphism, and $\mathrm{Im}\,\pi_i = \mathrm{Inn}(T) \cong T$ since $B \cap C \leq M$. Let $M_i := \ker \pi_i$. If all the subgroups M_i were distinct, then Lemma 4.3A would show that $|M| = |T|^m$ contrary to the hypothesis that $M < B$. On the other hand, if all the M_i were equal, then $|M| = |\mathrm{Inn}(T)|$ contrary to the hypothesis that $B \cap C < M$. Hence we have a nontrivial equivalence relation $\equiv$ defined on Γ by

$$i \equiv j \iff M_i = M_j.$$

We claim that this is an S-congruence. Indeed, $A = BC$ and so $L = B(L \cap C)$. Thus, if $s \in S$, then there exists $x := (\sigma, \ldots, \sigma)s \in L \cap C$ for some $\sigma \in \mathrm{Aut}(T)$. Then (4.3) shows that for each $z := (\tau_1, \ldots, \tau_m) \in M$ we have

$$x^{-1}zx = (\sigma^{-1}\tau_{1'}\sigma, \ldots, \sigma^{-1}\tau_{m'}\sigma) \in M \quad \text{where } i' := i^s.$$

Therefore $z \in M_{i'} \iff x^{-1}zx \in M_i$ and, in particular, $M_i = M_j \iff M_{i'} = M_{j'}$. Thus each $s \in S$ preserves the relation $\equiv$. Since $\equiv$ is nontrivial, this shows that $k \geq 3$ and S is not primitive. Hence the existence of a subgroup M satisfying (4.3) implies that neither (i) nor (ii) holds.

The last statement of the theorem now follows from Lemma 4.5B. This completes the proof of the theorem. □

Exercises

4.5.5 Suppose that $G \leq Sym(\Omega)$ and that H is a transitive subgroup of G. Let $\alpha \in \Omega$. Show that G is primitive if and only if there is no subgroup M of H such that $H_\alpha < M < H$ and M is normalized by G_α. (This generalizes Exercise 2.5.8.)

4.5.6 Let T be a finite nonabelian simple group acting regularly on a set Δ, and let $U := \langle(1234)\rangle \le Sym(\Gamma)$ where $\Gamma := \{1,2,3,4\}$. With the notation of Theorem 4.5A we know that the group $G := T \ wr_\Gamma\ U$ acts imprimitively on Ω (where $|\Omega| = |\Delta|^3$). Find an explicit nontrivial G-congruence on Ω.

4.5.7 Show that a finite group of diagonal type is never 2-transitive.

4.5.8 Suppose T is a nonabelian simple group, and let N^* denote the set of all permutations of T of the form $a \mapsto x^{-1}a^\sigma y$ where $x, y \in T$ and $\sigma \in \mathrm{Aut}(T)$. Show that N^* is a group which is permutation isomorphic to the group N defined in Lemma 4.5B in the case $m = 2$.

4.5.9 It is known that there exist infinite simple groups in which every two nonidentity elements are conjugate [see Higman et al. (1949)]. Suppose that T is such a group, and consider the group N^* defined in Exercise 4.5.8. Show that N^* is 2-transitive. (This shows that the condition "finite" cannot be dropped in Exercise 4.5.7.)

4.5.10 Let $H = T^m$ where T is a finite nonabelian simple group, and let π_i denote the projection of H onto the ith factor. Suppose that H acts transitively on a set Σ such that a point stabilizer $H_\alpha \cong T$ and, for each i, $\pi_i(H_\alpha) \neq 1$. Show that the action of H on Σ is equivalent to the diagonal action of H. [*Hint:* $\pi_i(H_\alpha) = T$ because H_α is simple.]

4.6 Finite Primitive Groups with Nonregular Socles

The socle H of a finite primitive group G is, according to Theorem 4.3C, either regular or else is the unique minimal normal subgroup of G. Section 4.7 deals with the case of a regular socle, while this section is devoted to the nonregular case. The main result is Theorem 4.6A which is the nonregular case of the O'Nan–Scott Theorem. In essence this theorem says that if the socle H is nonregular, then the primitive group G is either contained in the normalizer of a nonabelian simple group or else G is obtained from a primitive group of smaller degree via the product or diagonal constructions described in Sect. 4.3.

Corollary 4.3B shows that the socle H is always a direct product of copies of some simple group T; this group T will be called the *socle type* of G (so the socle type is determined up to isomorphism). As we observed before, since $H \lhd G$ and G is primitive, H is transitive, so G has nonabelian socle type whenever H is not regular.

Theorem 4.6A. *Let G be a finite primitive group with a nonregular socle and socle type T. Then G is permutation isomorphic to one of the following kinds of groups:*

(i) *a primitive group U with* $\mathrm{soc}(U) \cong T$*;*

(ii) *a primitive group U of diagonal type as described in Lemma 4.5B with* $\mathrm{soc}(U) \cong T^m$ *for some $m \geq 2$ (and degree $|T|^{m-1}$);*

(iii) *a primitive subgroup of a wreath product U wr_Γ $Sym(\Gamma)$ with the product action and $|\Gamma| > 1$, where U is a primitive nonregular group of one of the types (i) or (ii).*

Since $H := \mathrm{soc}(G)$ is nonregular, the centralizer $C_G(H) = 1$ in all cases (Theorem 4.3B), and so the conjugation action of G on H gives an embedding of G into $\mathrm{Aut}(H)$. In particular, classification of groups of type (i) reduces to the study of primitive permutation representations of groups G with $T \cong \mathrm{Inn}(T) \leq G \leq \mathrm{Aut}(T)$ for a finite simple group T; a group G of this kind is called *almost simple.* This reduces in turn to the classification of almost simple groups and their maximal subgroups. Groups of types (ii) and (iii) have nonsimple socles and are generally distinguished as having small orders with respect to their degrees.

PROOF OF THEOREM 4.6A. Let Ω be the set on which G acts, and consider the normalizer N of H in $Sym(\Omega)$. Since $G \leq N$, therefore N is also primitive. Since G has socle type T, we know that $H \cong T_1 \times \cdots \times T_m$ for some $m \geq 1$ where each $T_i \cong T$. If $m = 1$, then we have case (i). Thus we can suppose that $m \geq 2$, and proceed by induction on m.

Let $\pi_i : H \to T_i$ denote the projection of H onto the direct factor T_i. Let H_α be a point stabilizer of H, and put $R_i := \pi_i(H_\alpha) \leq T_i$. Since H is a normal subgroup of a primitive group, it is transitive on Ω and so $N = N_\alpha H$. Moreover, N acts transitively on the set $\{T_1, \ldots, T_m\}$ by conjugation (Theorem 4.3A), and therefore N_α also acts transitively on this set. Since $H_\alpha = H \cap N_\alpha \lhd N_\alpha$, the definition of π_i shows that, for all $u \in H_\alpha$ and $x \in N_\alpha$, we have

$$x^{-1}\pi_i(u)x = \pi_j(x^{-1}ux) \quad \text{whenever } x^{-1}T_ix = T_j. \tag{4.4}$$

In particular, if $x \in N_\alpha$, then $x^{-1}T_ix = T_j$ implies that $x^{-1}R_ix = R_j$. Thus the subgroups $R_1, \ldots, R_m$ are conjugate under N_α, and so the subgroup $K := R_1 \times \ldots \times R_m$ is normalized by N_α (see Fig. 4.1). By the definition of R_i we have $H_\alpha \leq K \leq H$. We consider two cases according to whether R_1 is or is not a proper subgroup of T_1.

Case 1: $R_1 < T_1$

In this case $H_\alpha \leq K < H$. Since K is normalized by N_α, and N is primitive, therefore $N_\alpha K = N_\alpha$ or N. But $N_\alpha K = N$ implies that K is a normal subgroup of N; since H is minimal normal in N by Corollary 4.3C and $K < H$, this is impossible. Hence $N_\alpha K = N_\alpha$, and so $H_\alpha = K = R_1 \times \cdots \times R_m$.

Fix an isomorphism of T_1 onto T and let R be the corresponding image of R_1. It follows from condition (4.4) that there is an isomorphism of each T_i onto T such that R_i maps onto R. Choose a transitive permutation

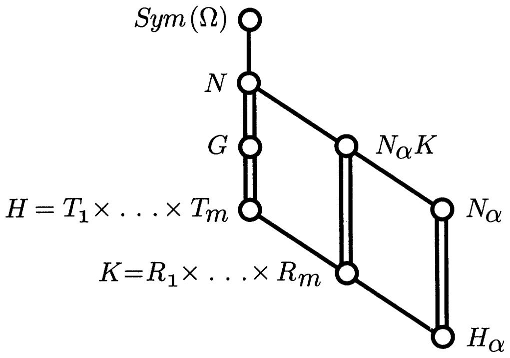


FIGURE 4.1. Subgroup lattice

representation of T on a set Δ, say, for which R is the stabilizer of a point δ, say. Then T^m acts transitively and faithfully on Δ^m via the product action; we shall identify T^m with its image in $Sym(\Delta^m)$. The point stabilizer in T^m of $(\delta, \ldots, \delta)$ is R^m, and it is clear that there is an isomorphism of H onto T^m such that H_α maps onto R^m. Hence $T^m \leq Sym(\Delta^m)$ is permutation isomorphic to $H \leq Sym(\Omega)$. Lemma 4.5A now shows that the normalizer N of H in $Sym(\Omega)$ is permutation isomorphic to a wreath product of the form $M \; wr_\Gamma \; S_m$ where $\Gamma := \{1, \ldots, m\}$ and M is the normalizer of T in $Sym(\Delta)$. Because N is primitive, Lemma 2.7A shows that M must also be primitive. Since $R \neq 1, T$ is not regular and $T \leq \mathrm{soc}(M)$. Since $\mathrm{soc}(M)$ is not regular, it is the unique minimal normal subgroup of M (Corollary 4.3B), so $T = \mathrm{soc}(M)$. This shows that M is a primitive group of the type described in (i), and hence G is permutation isomorphic to a group of the kind described in (iii). This completes the proof of the theorem in this case.

Case 2: $R_1 = T_1$

In this case the (conjugate) R_i equal T_i for all i. Thus H_α is a subdirect product of $H = T_1 \times \cdots \times T_m$, but not equal to H. Put $K_i := H_\alpha \cap \ker \pi_i$ for each i, and note that $H_\alpha / K_i \cong \pi_i(H_\alpha) = T_i$. Reindexing, if necessary, we may suppose that $K_1, \ldots, K_d$, say, are distinct, and every other K_i is equal to one of these. In particular, $K_1 \cap \cdots \cap K_d = 1$. Lemma 4.3A now shows that $H_\alpha = V_1 \times \cdots \times V_d$ where each $V_i \cong T$, and $d < m$ because $H_\alpha < H$. We divide the remaining argument into two subcases.

Subcase 2′: $R_1 = T_1$ *and* $d = 1$

In this case there is an isomorphism $\Psi : T \to H_\alpha$ and the composite mappings $\Psi_i := \pi_i \circ \Psi : T \to T_i$ are also isomorphisms. Hence $(t_1, \ldots, t_m) \mapsto \Psi_1(t_1) \cdots \Psi_m(t_m)$ is an isomorphism of T^m onto H which

maps the diagonal group

$$D := \{(t, \ldots, t) \mid t \in T\}$$

of T^m onto H_α (compare with Exercise 4.5.10). Hence H is permutation isomorphic to the base group of the wreath product considered in Lemma 4.5B. Since G normalizes H, the group G is therefore permutation isomorphic to a group of diagonal type (ii).

Subcase 2'': $R_1 = T_1$ and $d > 1$

In this final case we shall show that G is a group of type (iii). We have $H = T_1 \times \cdots \times T_m$ and $H_\alpha = V_1 \times \cdots \times V_d$ with $T_i \cong V_j \cong T$ for all i and j. We shall first show how the set of m factors of H can be partitioned into d blocks such that, for some group U having diagonal action, the direct product of the subgroups in each of the d blocks is isomorphic to $\mathrm{soc}(U)$.

We begin by noting that the subgroups V_j are the unique minimal normal subgroups of H_α, and

$$L_j := C_G(V_j) = \prod_{i \neq j} V_i \quad \text{for } j = 1, \ldots, d$$

are the unique maximal normal subgroups of H_α (see Exercise 4.3.6). On the other hand, since $\pi_i(H_\alpha) = T_i$ is a simple group, therefore $K_i = H_\alpha \cap \ker \pi_i$ is a maximal normal subgroup of H_α for each i. Thus we can define a partition $\{\Lambda_1, \ldots, \Lambda_d\}$ of $\Sigma := \{T_1, \ldots, T_m\}$ by

$$T_i \in \Lambda_j \iff K_i = L_j.$$

Note that each Λ_j is nonempty since $\cap K_i = 1$ while the intersection of any proper subfamily of the L_j's is not 1. Define U_j as the product of the subgroups in Λ_j for $j = 1, \ldots, d$. Clearly $H = U_1 \times \cdots \times U_d$. Moreover $U_j \cap H_\alpha = V_j$ since, if $x \in H_\alpha$, then

$$x \in U_j \iff \pi_i(x) = 1 \text{ for all } T_i \notin \Lambda_j \iff x \in \bigcap_{k \neq j} L_k = V_j.$$

As we just noted, N_α acts transitively by conjugation on Σ. On the other hand, it follows from condition (4.4) that, if $x \in N_\alpha$, then $x^{-1}K_i x = K_{i'}$ whenever $x^{-1}T_i x = T_{i'}$. Thus $\{\Lambda_1, \ldots, \Lambda_d\}$ is a set of blocks for this action. In particular, this shows that: $\{U_1, \ldots, U_d\}$ is a class of subgroups conjugate under N_α, each set Λ_j has size $s := m/d$, and $|U_j| = |T|^s$. Let Δ_i be the orbit of U_i which contains α for $i = 1, \ldots, d$. Since the U_i are conjugate under N_α, there exist elements $x_i \in N_\alpha$ such that $U_i = x_i^{-1}U_1 x_i$ and $\Delta_i = \Delta^{x_i}$ for each i where $\Delta = \Delta_1$. Thus the groups U_i are all permutation isomorphic to $U := U_1 \leq Sym(\Delta)$, and $|\Delta| = |U_1 : U_1 \cap H_\alpha| = |U_1 : V_1| = |T|^{s-1}$.

Since $V := V_1$ is equal to U_α, and $\pi_i(V) = T_i$ for each $T_i \in \Lambda_1$, Exercise 4.5.10 shows that the action of U on Δ is equivalent to the diagonal action. Let M be the normalizer of U in $Sym(\Delta)$; then Theorem 4.5A shows that M is a primitive group of the type described in (ii). Finally, define $W :=$

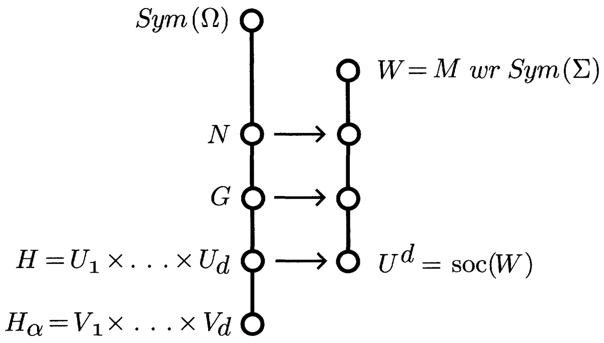


FIGURE 4.2. Subgroup lattice: subcase 2″

$M\ wr_\Sigma\ Sym(\Sigma)$ (see Fig. 4.2). Since the normalizer N of $H = U_1 \times \cdots \times U_d$ in $Sym(\Omega)$ contains G, it is primitive; therefore Lemma 4.5A shows that W is permutation isomorphic to N. Thus we conclude that G has the form described in part (iii), and the proof of the theorem is complete. □

The classification for the case of a nonregular socle which we have just completed can be summarized in a different way. We have shown that when the socle of a primitive group G is nonregular, then we can build the action of $\mathrm{soc}(G)$ by first taking a direct power $U = T^s$ of a simple group T with a transitive action ($s = 1$) or a diagonal action ($s \geq 2$), and then combining d copies of U with a product action. More precisely,

$$\mathrm{soc}(G) = T^{sd} \lhd G \leq [(T\ wr\ S_s) \ldots \mathrm{Out}(T)]\ wr\ S_d.$$

The case of a regular socle is addressed in the next section.

Exercises

4.6.1 Under what conditions is $\mathrm{soc}(G)$ primitive in Theorem 4.6A?

4.6.2 The Feit–Thompson Theorem [Feit and Thompson (1963)] states that every group of odd order is solvable. Using this theorem, show that if G is a finite primitive group of odd degree, then $\mathrm{soc}(G)$ is either simple or regular.

One natural question which arises is: when is the socle of a finite primitive group primitive? The question is easily answered when the socle is regular. The following example shows what may happen when the socle is nonregular and nonprimitive.

EXAMPLE 4.6.1. We introduced the Fano plane and its automorphism group $PSL_3(2)$ in Exercises 2.4.2 and 2.8.12. $PSL_3(2)$ is a simple group of order 168 which acts 2-transitively on the set of 7 points of the Fano plane and also on the set of 7 lines. Thus $PSL_3(2)$ acts transitively on the

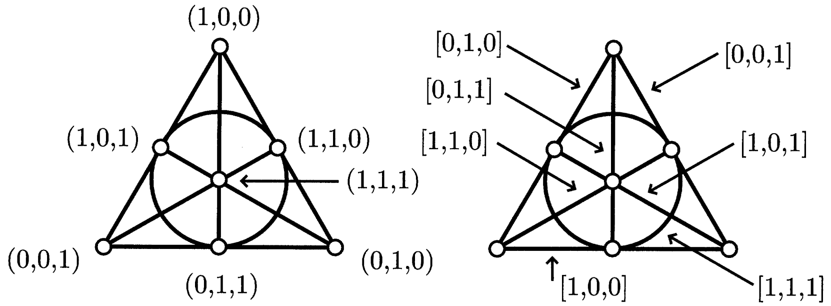


FIGURE 4.3. The Fano plane: point and line coordinates

set Δ of 21 incident point-line pairs (called "flags") and on the set Γ of 28 nonincident point-line pairs (called "antiflags"). Both of these actions are imprimitive (see Exercise 4.6.3).

Let $\mathbb{F}_2$ be the field of 2 elements. Then the points of the Fano plane can be labelled, as in Fig. 4.3, with the seven triples of coordinates from $\mathbb{F}_2$ which are not all zero. The lines can be similarly labelled with triples $[x, y, z]$ in such a way that the point (a, b, c) is incident with $[x, y, z]$ exactly when $ax + by + cz = 0$. (These are just the homogeneous coordinates for this projective plane.) Define a mapping τ (a "correlation") on the set of all points and all lines of the Fano plane by requiring τ to interchange each point (a, b, c) with the corresponding line $[a, b, c]$. Because τ preserves incidence, it acts as a permutation on each of the sets Δ and Γ, and so the group $L := \langle PSL_3(2), \tau\rangle$ acts transitively on both Δ and Γ. As the exercises below show, L acts primitively on both Δ and Γ, but its socle is nonregular and nonprimitive.

Exercises

4.6.3 Show that $PSL_3(2)$ acts imprimitively on each of Δ and Γ, and that in each case there are exactly two nontrivial congruences.

4.6.4 Show that $PSL_3(2)$ is the socle of L, and that L acts primitively and faithfully on both Δ and Γ.

4.6.5 (Continuation) Show that L has rank 4 on Δ, and rank 5 on Γ.

4.7 Primitive Groups with Regular Socles

In the preceding section we characterized finite primitive groups with nonregular socles. Here we will consider the case of a primitive group with a regular socle.

Let G be a finite primitive subgroup of $Sym(\Omega)$ whose socle H is regular, and let N be the normalizer of H in $Sym(\Omega)$. As before, we have $H \cong T^m$ for some simple group T and some integer $m \geq 1$, and $H \leq G \leq N$. Since N is the holomorph of H, Corollary 4.2B shows that $N \cong H \rtimes \mathrm{Aut}(H)$; more precisely, a point stabilizer N_α of N acting on Ω is permutation isomorphic to $\mathrm{Aut}(H)$ acting naturally on H, and $N = HN_\alpha$ with $H \cap N_\alpha = 1$. Similarly, $G = HG_\alpha$. We also note that G_α acts *irreducibly* on H in the sense that the only subgroups of H which are mapped into themselves under conjugation by G_α are 1 and H; indeed, if $1 < K < H$ and K is normalized by G_α, then $G_\alpha < KG_\alpha < G$ contrary to the maximality of G_α.

There are two quite distinct cases which have to be handled separately depending on whether H is abelian or nonabelian. If H is abelian, then Theorem 4.3B shows that H is an elementary abelian p-group for some prime p, the centralizer $C \leq N$ of H is equal to H and $\mathrm{soc}(N) = H = C = \mathrm{soc}(G)$. As we shall see below, in this case our characterization reduces to a problem in linear algebra.

On the other hand, if H is nonabelian, then C is also regular with $C \cong H$, but $\mathrm{soc}(N) = H \times C \neq \mathrm{soc}(G)$ and $G \cap C = 1$ (see Theorem 4.3B). The normalizer N is primitive of diagonal type. Consider the homomorphism $\Psi : N \to \mathrm{Aut}(H)$ induced by the conjugation action of N on H. Clearly $\Psi(N_\alpha) = \mathrm{Aut}(H)$ because N is the holomorph of H, $\ker \Psi = C$, and HC is the preimage of $\mathrm{Inn}(H)$ under Ψ. Since $HC \cap G = H(C \cap G) = H$, we conclude that $\Psi(G_\alpha) \cap \mathrm{Inn}(H) = 1$. Thus G_α is isomorphic to a subgroup of $\mathrm{Out}(H) = \mathrm{Aut}(H)/\mathrm{Inn}(H)$. Writing $H = T^m$ where T is a nonabelian simple group, Exercise 4.3.9 shows that

$$\mathrm{Out}(H) \cong (\mathrm{Aut}(T)\ wr_\Gamma\ S_m)\,/\,\mathrm{Inn}(T)^m \cong \mathrm{Out}(T)\ wr_\Gamma\ S_m$$

where $\Gamma = \{1, \ldots, m\}$. As we shall see in Theorem 4.7B, this condition on G_α is quite severe, and for some choices of T and m there are no corresponding primitive groups.

Exercises

4.7.1 Let K and H be arbitrary groups, and suppose that K acts faithfully and irreducibly as a group of automorphisms of H, and that no nontrivial element of K acts as an inner automorphism of H. Show that G acts faithfully and primitively by right multiplication on the set of right cosets of K and that H is the socle of $G := H \rtimes K$. (Of course, in the finite case, this can only happen when H is a direct product of simple groups.)

4.7.2 (Continuation) Suppose K and L are subgroups of $\mathrm{Aut}(H)$ and both act irreducibly on H. Show that the corresponding groups $H \rtimes K$ and $H \rtimes L$ are permutation isomorphic exactly when K and L are conjugate in $\mathrm{Aut}(H)$.

4.7.3 (Continuation) Show that the action of G on the set of right cosets of K is equivalent to the action of G on H defined by: $a^{(u,x)} := (au)^x$ where $a \in H$ and $(u,x) \in H \rtimes K$.

4.7.4 Let H be an elementary abelian p-group of order p^k for some prime p. Show that $\mathrm{Aut}(H) \cong GL_k(p)$, the *general linear group* of all invertible $k \times k$ matrices over the field $\mathbb{F}_p$ of p elements. [*Hint:* H is isomorphic to the additive group of a k-dimensional vector space V over $\mathbb{F}_p$. Show that $\mathrm{Aut}(V,+)$ is equal to the group $GL(V)$ of all invertible linear transformations on V.]

The next result follows immediately from the discussion above and Exercises 4.7.1 and 4.7.4.

Theorem 4.7A. *Let G be a finite primitive group with an abelian socle (which is necessarily regular). Then G has degree p^k for some prime p and some $k \geq 1$. If V is a vector space of dimension k over the field $\mathbb{F}_p$ with p elements, then there is a subgroup $K \leq GL(V)$ acting irreducibly on V and an isomorphism of G onto $V \rtimes K$ in which a point stabilizer of G maps onto K.*

In particular, it follows that (up to permutation isomorphism) the affine group $AGL_k(p)$ described in Sect. 2.8 is the unique maximal primitive group of degree p^k with abelian socle. Since quite a lot is known about the irreducible subgroups of $GL(V)$, Theorem 4.7A and Exercises 4.7.2 and 4.7.3 give a recipe for constructing the corresponding primitive groups for small degrees. Some references at given at the end of the chapter.

Exercises

4.7.5 Find all irreducible subgroups of $GL_2(3)$ and $GL_2(5)$ up to conjugacy, and use this information to find all primitive groups of degrees 3^2 and 5^2 with abelian socles.

4.7.6 Let E and F be finite fields with $|E| = |F|^m$. Show that $GL_n(E)$ is isomorphic to an irreducible subgroup of $GL_{mn}(F)$. In particular, $GL_m(F)$ contains an irreducible subgroup isomorphic to the multiplicative group of E.

4.7.7 Let $q = p^m$ be a power of the prime p. Since the multiplicative group of any finite field is cyclic, the preceding exercise shows that $GL_2(q)$ has an irreducible cyclic subgroup A of order $q^2 - 1$. Show that the subgroup of order $q + 1$ in A is also irreducible.

4.7.8 Suppose that $m \geq 1$ is an integer, and p and r are primes such that r divides $p^m - 1$ but r does not divide $p^k - 1$ for $1 \leq k <$ m. Show that $GL_m(p)$ has an irreducible cyclic subgroup of order r. (A theorem of K. Zsigmondy shows that a prime r satisfying these conditions exists for all p and m except for $p = 3$ and $m = 2$; see for example Lüneburg (1981).)

We finally turn to the case where the primitive group has a nonabelian regular socle. To obtain more precise results here we shall appeal to the "Schreier Conjecture" made by O. Schreier in 1926:

for every finite simple group T,

$$\mathrm{Out}(T) = \mathrm{Aut}(T)/\,\mathrm{Inn}(T) \text{ is solvable.}$$

To date this conjecture has only been proved using the classification of finite simple groups (see Appendix A) and a case-by-case examination of the various classes of simple groups. Actually, the classfication shows that much more is true: in many cases the group of outer automorphisms of a finite simple group is cyclic or even trivial, and in all cases it has a normal series of the form: $A \lhd B \lhd C$ where A is abelian, B/A is cyclic and $C/B \cong 1, S_2$ or S_3.

Theorem 4.7B (Assuming the Schreier Conjecture for T). *Let $G \leq Sym(\Omega)$ be a finite primitive group with a regular nonabelian socle $H = T_1 \times \cdots \times T_m$ where each of the factors T_i is isomorphic to a finite nonabelian simple group T and $m \geq 1$. Let G_α be a point stabilizer of G. Then the following hold.*

(i) *G_α has no nontrivial solvable normal subgroup.*
(ii) *The action of G_α by conjugation on the set $\{T_1, \ldots, T_m\}$ (see Theorem 4.3A) is transitive and faithful, so G_α is isomorphic to a transitive subgroup of S_m.*
(iii) *In the action of G_α defined in (ii), the stabilizer $N_{G_\alpha}(T_1)$ of T_1 contains a composition factor isomorphic to T.*
(iv) *The integer m must be large enough so that T is isomorphic to a section of S_{m-1}. In particular, $m \geq 6$ for all T.*

PROOF. (i) Suppose that G_α had a nontrivial normal solvable subgroup. Then Theorem 4.3A shows that G_α has a minimal normal subgroup P which is an elementary abelian p-subgroup for some prime p. Because G_α is maximal in G, therefore $N_G(P) = G_\alpha$ and so, in particular, $C_H(P) = 1$. Thus, in the action of P by conjugation on H, $\{1\}$ is the only orbit of length 1. Since every nontrivial orbit of P has length divisible by p, we conclude that p divides $|H| - 1$, and p does not divide $|H|$.

On the other hand, if q is a prime dividing $|H|$, then the number n_q of Sylow q-subgroups of H divides $|H|$ and so p does not divide n_q. Now P acts on the set of Sylow q-subgroups of H by conjugation; since p does not divide n_q, at least one of the orbits in this action has length 1. Thus we conclude that some Sylow q-subgroup Q of H is normalized by P. We claim that Q is the only Sylow q-subgroup normalized of H by P. Indeed, suppose that P also normalizes $u^{-1}Qu$ for some $u \in H$. Then P and uPu^{-1} are both Sylow p-subgroups in $N_{HP}(Q)$. Thus, for some $v \in H \cap N_{HP}(Q)$, we have $vuPu^{-1}v^{-1} = P$, and so $vu \in G_\alpha \cap H = 1$. Hence $u \in N_{HP}(Q)$, and so $u^{-1}Qu = Q$. This shows that Q is the unique Sylow q-subgroup of H

normalized by P. Therefore $z^{-1}Pz = P$ implies $z^{-1}Qz = Q$, and so Q is normalized by G_α. Hence $H = Q$ because G_α acts irreducibily on H. This contradicts the hypothesis that H is a product of nonabelian simple groups. Thus G_α has no nontrivial normal abelian subgroup, and (i) is proved.

(ii) G_α acts by conjugation on the set $\{T_1, \dots, T_m\}$ because these are the only minimal normal subgroups of H by Theorem 4.3A. Let K be the kernel of this action. As we noted at the beginning of this section, the action of conjugation of G_α on H defines an embedding Ψ of G_α into $\mathrm{Aut}(H)$ such that $\Psi(G_\alpha) \cap \mathrm{Inn}(H) = 1$. Then $K \cong \Psi(K) \leq \mathrm{Aut}(T_1) \times \dots \times \mathrm{Aut}(T_m)$ with $\Psi(K) \cap (\mathrm{Inn}(T_1) \times \dots \times \mathrm{Inn}(T_m)) = 1$. Since $\mathrm{Out}(T_i) = \mathrm{Aut}(T_i)/\mathrm{Inn}(T_i)$ is solvable by the Schreier Conjecture for T, K must also be solvable, and so $K = 1$ by (i). This shows that the given action of G_α on $\{T_1, \dots, T_m\}$ is faithful, and it is transitive because G_α acts irreducibly on H. Thus G_α is isomorphic to a transitive subgroup of S_m.

(iii) Put $L := N_G(T_1)$ and $C := C_G(T_1)$. Since $T_2 \times \dots \times T_m \leq C$ we have $H \leq T_1C$ and $L = HL_\alpha = T_1L_\alpha C$. Note that L_α is the stabilizer in G_α of the point T_1 in the action described in (ii).

Put $K := L_\alpha C$. If $K = L$, then $T \cong HC/C \lhd L/C = L_\alpha C/C \cong L_\alpha/(L_\alpha \cap C)$ and the conclusion of (iii) follows. It remains to consider the case where $K < L$.

Suppose that $K < L$, and choose M maximal in L such that $K \leq M < L$. Put $U_1 := M \cap T_1$ and note that L_α normalizes U_1; we claim that $U_1 = 1$. Indeed, since L_α is the stabilizer of T_1 in the action in (ii), $G_\alpha = \bigcup_{1 \leq i \leq m} L_\alpha x_i$ where $x_i^{-1}T_1x_i = T_i$ for $i = 1, \dots, m$. Hence, putting $U_i := x_i^{-1}U_1x_i$, we see that $U_1 \times \dots \times U_m$ is a subgroup of H which is normalized by G_α. Since G is primitive, G_α acts irreducibly on H, and so $U_1 \times \dots \times U_m = 1$ or H. Hence $U_1 = 1$ or T_1. The latter alternative cannot hold because if $T_1 < M$ then $H \leq T_1C < M$ so $HL_\alpha = L \leq M < L$. So $U_1 = M \cap T_1 = 1$ as claimed.

Now, since $K \leq M$, we have $M = M \cap T_1K = (M \cap T_1)K = K$, and so $M = K$. Thus K is maximal in L, $L = T_1K$, $T_1 \lhd L$ and $T_1 \cap K = 1$. Consider the action of L by right multiplication on the set of right cosets of K in L, and let $\overline{L}$ denote the image of this action. Since $C \leq K$ and is normal in L, the point stabilizer $\overline{K}$ of $\overline{L}$ is a homomorphic image of $K/C = L_\alpha C/C \cong L_\alpha/(L_\alpha \cap C)$. Moreover, $\overline{L}$ is primitive because K is maximal in L, and the image $\overline{T_1}$ of T_1 is a regular normal subgroup isomorphic to T. Now Theorem 4.3B shows that $\mathrm{soc}(\overline{L})$ is either $\overline{T_1}$ or $\overline{T_1} \times \overline{C_1}$ where $\overline{C_1} \cong \overline{T_1}$. In the former case we are in the situation of the present theorem with $m = 1$; (ii) shows that this is impossible because a primitive nonabelian group cannot be regular. In the latter case, the point stabilizer $\overline{K}$ of $\overline{L}$ must contain a normal subgroup isomorphic to $\overline{C_1}$ because $\overline{T_1}$ is regular. Since $\overline{K}$ is a homomorphic image of L_α, this implies that L_α contains a composition factor isomorphic to T as required. This completes the second case.

(iv) This follows immediately from (iii) and the fact that S_4 has no simple nonabelian sections. □

An alternative approach to describing finite primitive groups with nonabelian regular socles is through the construction of the *twisted wreath product* first introduced in Neumann (1963). The construction of the twisted wreath product in general may be explained as follows.

Let T and K be arbitrary groups and let L be a subgroup of K together with a specified homomorphism $\varphi : L \to \mathrm{Aut}(T)$. Let R be a set of left coset representatives for L in K. Recall that the set $\mathrm{Fun}(K,T)$ of all functions $f : K \to T$ is a group under pointwise multiplication (see Sect. 2.6). We can define an action of K on $\mathrm{Fun}(K,T)$ preserving this group operation via $f^x(z) := f(xz)$ ($f \in \mathrm{Fun}(K,T), x, z \in K$). Now define $H \subseteq \mathrm{Fun}(K,T)$ to consist of all $f \in \mathrm{Fun}(K,T)$ such that $f(zy) = f(z)^{\varphi(y)}$ for all $z \in K$ and $y \in L$. It is readily verified that H is a subgroup of $\mathrm{Fun}(K,T)$ which is invariant under the action of K and, moreover, the restriction mapping $f \mapsto f\mid_R$ is an isomorphism of H onto $\mathrm{Fun}(R,T)$ (see Exercises 4.7.9 and 4.7.10 below). In particular, if $|R| = |K : L| = m$, say, this shows that $H \cong T^m$. Thus we can define the semidirect product $G = H \rtimes K$. This is called the twisted wreath product with respect to the data (T, K, φ), and may be compared with the wreath product defined in Sect. 2.6.

Exercises

4.7.9 With the notation above show that H is a subgroup of $\mathrm{Fun}(K,T)$ and that there is an action of K on H preserving the group operation given by $f^x(z) = f(xz)$ ($x, z \in K$ and $f, f^x \in H$).

4.7.10 (Continuation) Show that the restriction mapping $f \mapsto f\mid_R$ is an isomorphism of H onto $\mathrm{Fun}(R,T)$ and that $\mathrm{Fun}(R,T) \cong T^m$ when $|R| = m$.

It can be shown that any finite primitive group with a regular nonabelian socle of the form T^m (T simple) is isomorphic to a twisted wreath product (T, K, φ) where $|K : L| = m$ and $\varphi : L \to \mathrm{Aut}(T)$ has $\mathrm{Im}\,\varphi \geq \mathrm{Inn}(T)$ (see Liebeck et al. 1988a). However, there seems to be no known simple necessary and sufficient conditions on T, K and φ for this twisted wreath product to satisfy the criteria of Exercise 4.7.1 and hence represent a finite primitive group. The following lemma gives a useful, easily applicable sufficient condition.

Lemma 4.7A. *Let T be a finite nonabelian simple group, and $K \leq S_m$ be a primitive permutation group with point stabilizer L. Suppose that $\varphi : L \to \mathrm{Aut}(T)$ is a homomorphism such that* $\mathrm{Im}\,\varphi \geq \mathrm{Inn}(T)$, *but* $\mathrm{Im}\,\varphi$ *is not a homomorphic image of K. Then the twisted wreath product $G = H \rtimes K$ defined above using the data (T, K, φ) satisfies the conditions of Exercise*

4.7.1. Thus G is isomorphic to a primitive group with regular socle T^m and point stabilizer isomorphic to K.

PROOF. Let R be a set of left coset representatives of L in K with $1 \in R$. We shall first show that no nontrivial $x \in K$ induces an inner automorphism of H. Indeed, since L is a point stabilizer of K, therefore $\bigcap_{r \in R} rLr^{-1} = 1$, and so $x \notin rLr^{-1}$ for some $r \in R$. This implies that $xr = sy$ for some $y \in L$ and $s \in R$ with $s \neq r$. Now, since the restriction $f \mapsto f\mid_R$ is an isomorphism of H onto $\mathrm{Fun}(R,T)$, we can choose $f \in H$ such that $f(r) = 1$ and $f(s) \neq 1$. Then for each $g \in H$ we have $g^{-1}(r)f(r)g(r) = 1$ while $f(xr) = f(sy) = f(s)^{\varphi(y)} \neq 1$, which shows that the action of x on H is not an inner automorphism. Thus no nontrivial element of K induces an inner automorphism on H and, in particular, K acts faithfully on H.

It remains to show that K acts irreducibly on H. Let M be a minimal K-invariant subgroup of H with $M > 1$; we have to show that $M = H$. For each $r \in R$ we have the homomorphism $\pi_r : M \to T$ given by $f \mapsto f(r)$. Taking $x = rs^{-1}$ we have $f(r) = f^x(s)$ for any $f \in M$ and $r, s \in R$. Since M is K-invariant, this shows that $\mathrm{Im}\,\pi_r = \mathrm{Im}\,\pi_s$ for all r and s. Let T_0 denote this common image, and note that $T_0 \neq 1$ because $M \neq 1$. Taking $x = ryr^{-1}$, we have $f(r)^{\varphi(y)} = f(ry) = f(xr) = f^x(r) \in T_0$ for all $y \in L$ and $r \in R$. Since $\mathrm{Im}\,\varphi \geq \mathrm{Inn}(T)$, this shows that $1 \neq T_0 \triangleleft T$ and so $T_0 = T$ by the simplicity of T. To prove that $M \cong T^m$ (and hence $M = H$), it is enough to show that the kernels of the π_r are distinct (see Lemma 4.3A).

Suppose on the contrary that $\ker \pi_r = \ker \pi_s = M_0$, say for some $r \neq s$ where $M_0 < M$. Let $f \in M_0$. Then taking $x = ryr^{-1}$ with $y \in L$, we have $f^x(r) = f(ry) = f(r)^{\varphi(y)} = 1$. Similarly, taking $x = sr^{-1}$ we find that $f^x(r) = f(s) = 1$. Thus M_0 is invariant under $\langle rLr^{-1}, sr^{-1}\rangle$, and the latter equals K because L is maximal in K. Now the choice of M shows that $M_0 = 1$, and so $\ker \pi_1 = 1$ and $M \cong \mathrm{Im}\,\pi_1 = T$. The image of the action ψ of K on M is contained in $\mathrm{Aut}(M)$ because K preserves the group operation. Since $f^y(1) = f(1)^{\varphi(y)}$ for all $f \in M$ and $y \in L$, the image of ψ restricted to L is isomorphic to $\mathrm{Im}\,\varphi$ and contains $\mathrm{Inn}(M)$. Because L contains no nontrivial normal subgroup of K, we conclude that ψ is not faithful, and so the maximality of L in K shows that $K = (\ker \psi)L$. But then $K/\ker \psi \cong \mathrm{Im}\,\psi = \psi(L) \cong \mathrm{Im}\,\varphi$ which contradicts one of the hypotheses of the lemma. Thus the mappings π_r have distinct kernels, and H is irreducible as claimed. This completes the proof of the lemma. □

Exercises

4.7.11 Show that there exist primitive groups which have regular socles isomorphic to $(A_5)^m$ for $m = 6$, 21 and 56. Does there exist one when $m = 7$?

4.7.12 Show that for any finite simple group T there is a primitive group with a regular socle isomorphic to $T^{|T|}$.

4.7.13 Let K be a simple normal subgroup of a finite group G with $G' = G$. Assuming the Schreier Conjecture, show that $G = K \times C_G(K)$.

4.8 Applications of the O'Nan–Scott Theorem

The main focus of this chapter has been the proof of the O'Nan–Scott Theorem, Theorem 4.1A. Since the argument was spread over several sections, the overall picture may have been obscured. In this final section we shall summarize this important result and describe a few of its significant applications.

A finite primitive group G has a socle $H \cong T^m$ which is the direct product of m copies of some simple group T (Corollary 4.3B). The analysis then divides into two cases depending on whether or not H is regular. Let n denote the degree of G.

If the socle H is regular then one of the following cases holds.

(i) *Affine type:* H is an elementary abelian p-group, $n = p^m$, and G is a subgroup of the affine group $AGL_m(p)$ containing the translations. The stabilizer G_α is an irreducible subgroup of $GL_m(p)$ (Theorem 4.7A).

(ii) *Regular nonabelian type:* H and T are nonabelian, $n = |T|^m$, $m \geq 6$ and the group G can be constructed as a twisted wreath product. The stabilizer G_α is tightly constrained and in particular is isomorphic to a transitive subgroup of S_m whose point stabilizers have a composition factor isomorphic to T (Theorem 4.7B).

If the socle H is not regular then H is nonabelian and one of the following cases holds (Theorem 4.6A).

(iii) *Almost simple type:* H is simple and $G \leq \mathrm{Aut}(H)$; G/H is solvable by the Schreier Conjecture.

(iv) *Diagonal type:* $H = T^m$ with $m \geq 2$, $n = |T|^{m-1}$ and G is a subgroup of a wreath product with the diagonal action. The stabilizer satisfies $\mathrm{Inn}(T) \leq G_\alpha \leq \mathrm{Aut}(T) \times S_m$ and has a primitive action of degree m. (See Lemma 4.5B.)

(v) *Product type:* $H = T^m$ with $m = rs$ and $s > 1$. There is a primitive, nonregular group U with socle T^r and of type (iii) or (iv) such that G is isomorphic to a subgroup of the wreath product $U \ wr \ S_s$ with the product action. The degree of G is $n = (d)^s$ where d is the degeee of U.

With the O'Nan–Scott Theorem available, a problem about a finite primitive group G can be broken up into these five cases. In a typical situation, we can deal with the case of a regular normal subgroup in a straightforward way. If G is of diagonal type we have a detailed description of the action, while if G is of product type a strong inductive setup is available.

So often a problem can be reduced to the case of a group G of almost simple type. At this point we turn to the large body of detailed knowledge available about finite simple groups. In particular, using the classification of finite simple groups, we can consider the separate types of finite simple group as possible socles for G. Of course, in a particular problem any or all of these steps may be nontrivial, but the O'Nan–Scott Theorem does provide an effective framework for using detailed information about finite simple groups to answer significant questions about finite primitve groups. The rest of this section sketches a few of the results obtained by using the O'Nan–Scott Theorem. For further discussion see, for example, Cameron (1981a) and Praeger (1990).

(A) Listing Primitive Groups

The analysis of primitive groups in terms of their socles provides a natural approach to listing the primitive groups. For example, Appendix B contains a list of all the primitive groups of degree less than 1000. Taking a more general approach, Liebeck and Saxl (1985b) list all primitive groups of odd degree. These lists were constructed in the following way. If G is primitive on Ω then the socle H is transitive and $H \triangleleft G \leq Sym(\Omega)$. Each list item is essentially a transitive action for a particular socle H along with information about the structure of G_α and the normalizer of H in $Sym(\Omega)$. In Dixon and Mortimer (1988) such a list item is called a *cohort* of groups. The permutation groups in one cohort all have the same socle with a specified action. There are 762 cohorts of proper primitive groups of degree less than 1000.

A primitive group G has a socle $H = T^m$ for some simple group T. If H is abelian then G_α is an irreducible subgroup of $GL_m(p)$ and we do not explore this case any further. In the case of a nonabelian regular socle, the degree of G is $|T|^m$ where $m \geq 6$. Since the order of a nonabelian simple group is even and at least 60, the degree of G is even and at least $60^6 > 1000$. Thus neither of the lists includes any primitive groups of this type. The degree of a group G of diagonal type is also a power $|T|^{m-1}$ of the order of a nonabelian simple group and hence is even. The primitive groups of this type with degrees less than 1000 have $m = 2$ and $T = A_5, A_6, PSL_2(7), PSL_2(8)$, or $PSL_2(11)$.

If G is of product type then the degree of G is a power d^k, with $k \geq 2$, where d is the degree of some other primitive group U. The group G has odd degree when U has odd degree. The condition $d^k < 1000$ requires $k = 3$ and $d < 10$, or $k = 2$ and $d < 32$. Thus the groups of product type give an inductive class of examples in each list. There are 74 cohorts of groups with socles of this type and degree less than 1000.

The largest class of examples on both lists consists of the groups with a simple nonabelian socle. For these groups, we need information about

the maximal subgroups of the almost simple groups. Concerted efforts by a number of mathematicians over the past century have provided enough information to deal with this case.

(B) Degree and Rank

The O'Nan–Scott Theorem shows that a primitive group which is not of almost simple type has a degree which is a power of the order of a finite simple group or a nontrivial power d^k of the degree d of some other primitive group. Thus the degrees that actually occur for proper primitive groups are a relatively sparse set of natural numbers. There are 486 degrees $n < 1000$ such that the only primitive groups of degree n are A_n and S_n. Let E be the set of all n for which there is a proper primitive group of degree n. Then E is the union of the following sets:

$E_1 := \{p \mid p \text{ prime}, p \geq 5\}$;
$E_2 := \{m^k \mid m \geq 2, k \geq 2, m^k > 4\}$;
$E_3 := \{n \mid \text{ there is a nonabelian simple group of order } n\}$;
$E_4 := \{d \mid$ there is a proper primitive group G of degree d whose socle is simple and nonabelian $\}$.

The density of each of these sets can be estimated. The sets E_1 and E_2 involve only properties of the integers and we only need the orders of the finite simple groups to deal with set E_3. On the other hand, many detailed facts about finite simple groups are required to estimate the density of the set E_4. Calculating these densities, Cameron et al. (1982) obtained the following asymptotic estimate for the density of E. Let $\pi(x)$ denote the number of prime numbers $p \leq x$.

Theorem 4.8A. *If $e(x)$ is the number of degrees $n \leq x$ such that there is a proper primitive group of degree n then*

$$e(x) = 2\pi(x) + (1+\sqrt{2})x^{\frac{1}{2}} + O\left(\frac{x^{\frac{1}{2}}}{\log x}\right) \sim \frac{2x}{\log x}.$$

As another example of the reduction of a problem to the almost simple case, consider the question of rank. Suppose that G is a primitive permutation group with a nonabelian socle $H = T^m$ with T simple. Then the rank r of G satisfies $r \geq m+1$. This follows from the bound in Exercise 4.8.1 if G has product type or from Exercise 4.8.2 if H is regular. A similar bound for groups of diagonal type is proved in Cameron (1981a).

When studying a 2-transitive group G, these lower bounds on the rank show that either G is almost simple, or else G is an affine group; this proves Theorem 4.1B. (See also Exercise 4.5.7.) The analysis then shifts, on the one hand, to examining the 2-transitive actions of the almost simple groups

and, on the other hand, to determining the subgroups of $GL_m(p)$ that act transitively on the set of nonzero vectors in the underlying vector space. In this way, the finite 2-transitive groups have been completely determined; see Sect. 7.7 for a more detailed discussion.

(C) The Sims Conjecture

Suppose that G is a primitive group of degree n acting on a set Ω. The subdegrees of G are the lengths of the orbits of the stabilizer G_α. Consider the primitive groups with a given subdegree $d > 1$. For a fixed d there is no immediate bound on the degree n of G. For example, for any prime p the dihedral group D_{2p} has a representation as a primitive permutation group of degree p with a subdegree $d = 2$. On the other hand, as we saw, for example, in Sect. 3.2 and 4.4, a small subdegree does strongly restrict the structure of G_α. Following his investigation of the cases $d = 3$ and $d = 4$, C. Sims was lead to conjecture the following theorem (see Exercise 4.4.11). It was finally proved using the O'Nan–Scott Theorem and the classification of finite simple groups [see Cameron et al. (1983)].

Theorem 4.8B. *There is a function f such that if G is a finite primitive group with a suborbit of length $d > 1$ then the pointwise stabilizers have order at most $f(d)$.*

The simplest case in proving the Sims Conjecture is when G is a primitive group with a regular socle H. We can identify Ω with the elements of H in such a way that G_α acts on H by conjugation in the same way it acts on Ω. Since G is primitive there are no nontrivial G_α-invariant subgroups of H. Thus the group generated by the elements of H in any nontrivial orbit of G_α is H itself. In particular, G_α acts faithfully on each of its orbits and hence has order at most $d!$. This establishes the result in the case of a regular socle.

If G is of diagonal type then an analysis of the action itself, without using specfic properties of the simple group T, shows that $|G_\alpha| \leq (d!)^{d+1}$ in this case. If G is a primitive group of product type then G is permutation isomorphic to a subgroup of a wreath product of the form $U \text{ } wr \text{ } S_b$ where U is primitive on a set Δ and is of almost simple or diagonal type. Suppose $\delta \in \Delta$. Then it can be shown that $|G_\alpha| \leq |U_\delta|^d d!$. Thus if we assume that there is an increasing function $h(d)$ making Theorem 4.8B true for all groups G with a simple socle then we can define a function $f(d)$ that will work for all primitive groups. The proof of Theorem 4.8B is then completed by dealing with the almost simple case and using key results of Thompson (1970) and Wielandt (1971a) about the subgroup structure of G_α. This is the most complicated part of the proof and uses specific information about various simple groups. The function $f(d)$ can be taken of the form $\exp(d^2 o(d))$ though this is not best possible.

Exercises

4.8.1 Suppose that G is a primitive subgroup of the wreath product $U\ wr\ S_b$ where U is a primtive group with rank r_0. Show that the rank of G is at least $\binom{r_0+b-1}{b} \geq b+1$.

4.8.2 Suppose that G is primitive with a nonabelian regular socle $H = T^m$. Show that G has rank at least $m+1$.

4.9 Notes

- Theorem 4.1B: This result is an early precursor of the O'Nan–Scott Theorem which appears in Burnside (1911) §154 with a proof based on the Frobenius Theorem (see Sect. 7.2). The O'Nan–Scott Theorem (Theorem 4.1A) itself was announced at the Santa Cruz Conference on Finite Groups in 1979 by M. O'Nan and L.L. Scott [see Scott (1980)] in a slightly incomplete form which is repeated in Cameron (1981a). A proof of part of this theorem appears in Hoffmann (1982), but the first complete published proofs appear in Buekenhout (1988) and Liebeck et al. (1988a). For related papers, see Aschbacher and Scott (1985), Kovács (1986) and (1989), and Baddeley (1993).
- Sect. 4.2: This material is classical.
- Exercise 4.2.14: The construction of an infinite group with two conjugacy classes (the group is necessarily torsion-free) is based on the HNN-construction of Higman et al. (1949). This construction is also given in Rotman (1995), Exercise 12.63 and in Cohen (1989) Prop. 38 (and the following comment there).
- Exercise 4.2.16: See Mills (1953).
- Corollary 4.2B: See Wielandt (1967a) for a related result.
- Exercise 4.2.17: See Neumann (1987).
- Sect. 4.3: The word "socle" is an architectural term which refers to a support beneath the base of a column. Material of this section is classical.
- Exercise 4.3.14: See Fisher (1975).
- Sect. 4.4: The theory of subnormal subgroups is extensive [see Lennox and Stonehewer (1986)]; and many of the basic results are due to Wielandt [see Wielandt (1971a), (1971b) and (1994)]. Some of the exercises at the end of this section deal with special cases of "Sim's Conjecture"; see Sect. 4.8 for further details.
- Lemma 4.4B: See Szep (1953).
- Theorem 4.4A: See Wielandt (1962), (1971a).
- Exercise 4.4.4: See Goldschmidt and Scott (1978).
- Exercise 4.4.9: See Knapp (1981).
- Exercise 4.4.11: See Sims (1967) and Wong (1967).
- Sect. 4.5: See Kovács (1989) for further details about primitive wreath products.

- Theorem 4.7A: Abelian socles seem to be quite different from nonabelian socles, and different techniques are required to analyze them. Short (1992) describes very clearly a general method of constructing the primitive groups with abelian socles; the general ideas go back to Jordan. Dornhoff (1969), Foulser (1969), and Seager (1987) and (1988) deal with finite solvable primitive groups of low rank, following the classification by Huppert (1957) of finite 2-transitive solvable groups. Liebeck (1986) classifies the primitive affine groups of rank 3.
- Exercise 4.7.8: Zsigmondy's Theorem is a useful theorem worth knowing. Proofs can be found in Lüneberg (1981) and in Lüneberg (1980) Theorem 6.2. See also Huppert and Blackburn (1982a).
- Sect. 4.8: Much has been done to compute primitive groups of small degree. See for example, Cooperstein (1978), Kantor (1979), and Pogorelov (1980). The list of primitive groups in Dixon and Mortimer (1988) is reprinted as Appendix B to this book [see also Il'in and Takmakov (1986)].

For other applications of the classification of finite simple groups to permutation groups, see Kantor (1985a), (1985b) and (1987); Kantor and Liebler (1982); Liebeck (1984b); Liebeck and Saxl (1985a), (1986) and (1991); and Liebeck et al. (1987) and (1988b).

5

Bounds on Orders of Permutation Groups

The theme of the present chapter is use of combinatorial methods to bound the order of various classes of subgroups of the finite symmetric groups. Typically we find that, excluding A_n and S_n themselves, the larger subgroups of S_n are either intransitive or imprimitive (Theorem 5.2B). On the other hand, the proper primitive groups are all quite small; we shall show that a proper primitive group of degree n that is not 2-transitive has order at most $\exp(4\sqrt{(n)}(\log n)^2)$ (Theorem 5.3A) while a proper 2-transitive group of degree n has order at most $\exp(72(\log n)^3)$ (Theorem 5.6A). To obtain these results we are naturally led to a study of the orders of elements and properties of bases and minimal degrees.

5.1 Orders of Elements

We begin by looking at the orders of the simplest subgroups: the cyclic subgroups. Our object in this section is to give a lower bound to the largest order of an element in the alternating group A_n. It might seem more natural to look instead at the orders of elements in the symmetric group. Actually the results for the two groups are very closely linked (see Exercise 5.1.5), but for technical reasons we are more interested in the alternating group. The result is essentially a theorem in elementary number theory, and it begins with an estimate, made by P.L. Chebyshev in 1852, of the number theoretic function

$$\theta^*(z) := \sum_{2<p\leq z} \log p$$

for real positive z. Here, and for the rest of this section, p runs over the primes and log denotes the natural logarithm.

Lemma 5.1A. *$\theta^*(z) > z/2$ for all $z \geq 11$.*

PROOF. The result can be verified directly for small values of z (see Exercise 5.1.1 below), so we suppose that $z \geq 1270$. It is enough to show that $\theta^*(2n) \geq n+1$ for all integers $n \geq 635$, since then

$$\theta^*(z) \geq \theta^*(2\lfloor z/2 \rfloor) \geq \lfloor z/2 \rfloor + 1 > z/2.$$

We shall proceed by induction on n. Put $m = \binom{2n}{n}$ with $n \geq 635$. Then m is the value of the largest of the $2n+1$ binomial coefficients in the expansion of $(1+1)^{2n}$, and is also larger than the sum of the first and last coefficients. Hence we get the lower bound $2^{2n}/2n < m$. On the other hand, we can obtain an upper bound for m as follows. The largest power of a prime p which divides $n!$ is p^e where $e = \sum_{i=1}^{\infty} \lfloor n/p^i \rfloor$ (see Exercise 2.6.8). Therefore

$$\log m = \sum_{p \leq 2n} \delta(p) \log p$$

where

$$\delta(p) := \sum_{i \geq 1} \left\{ \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right\}.$$

It is readily verified that for any real number $\xi > 0$ we have $\lfloor 2\xi \rfloor = 2\lfloor \xi \rfloor$ or $2\lfloor \xi \rfloor + 1$, so each of the terms in the sum for $\delta(p)$ is either 0 or 1. Since all the terms are 0 when $p^i > 2n$, there are at most $\lfloor (\log 2n)/(\log p) \rfloor$ nonzero terms. Therefore

$$\delta(p) \leq 1 \quad \text{when } \sqrt{2n} < p \leq 2n,$$
$$\delta(p) \log p \leq \log 2n \quad \text{when } p \leq \sqrt{2n}.$$

Using these estimates and the inequality $m > 2^{2n}/2n$ obtained above:

$$2n \log 2 - \log 2n < \log m < \theta^*(2n) - \theta^*(\sqrt{2n}) + \sqrt{2n} \log 2n$$

which shows that

$$\theta^*(2n) - n - 1 > (2\log 2 - 1)n - (1 + \sqrt{2n}) \log 2n + \theta^*(\sqrt{2n}) - 1.$$

Now $\theta^*(\sqrt{2n}) > \sqrt{2n}/2$ by induction, and so elementary estimates show that the right hand side of the inequality above is greater than 0 (see Exercise 5.1.2 below). Thus $\theta^*(2n) > n+1$ and the induction step is proved. This proves the theorem. □

Exercises

5.1.1 Verify the values of θ^* in Table 5.1 and use it to prove that $\theta^*(z) > z/2$ for $11 \leq z < 1270$.

5.1.2 Prove that the right hand side in the last displayed inequality in the proof above is greater than 0 for all $n \geq 635$. [*Hint:* Replace $\theta^*(\sqrt{2n})$ by the lower bound $\sqrt{n/2}$, and show that the derivative of the resulting expression with respect to n is positive for $n \geq 635$.]

TABLE 5.1. Selected Values of $\theta^*(p)$

$p =$	11	13	19	29	43	71	113	211	383	709
$\theta^*(p) =$	7.1	9.6	15.4	21.9	36.4	60.9	106.4	193.2	358.1	678.9

It is known that $\theta^*(z)/z \to 1$ as $z \to \infty$. This fact is one form of the "Prime Number Theorem". A better known form of this theorem is that the number of primes less than z is asymptotic to $z/\log z$ [see for example, Apostol (1976)].

Theorem 5.1A. *If $n \geq 7$, then A_n contains an element of order greater than* $\exp\sqrt{\frac{1}{4}n\log n}$.

PROOF. Suppose that $p_1, \ldots, p_r$ are distinct odd primes such that $p_1 + \cdots + p_r \leq n$. Then A_n contains an element whose nontrivial cycles have lengths $p_1, \ldots, p_r$ and whose order is therefore $p_1 \cdots p_r$. Thus it is enough to show (with the notation above) that there exists a real number z such that

$$\sum_{2<p\leq z} p \leq n \quad \text{and} \quad \theta^*(z)^2 > \frac{1}{4}n\log n.$$

The small cases are easily verified (see Exercise 5.1.3 below) so we shall assume that $n \geq 22$. Put $F(z) := z/\log z$. Elementary calculus shows that F is an increasing function for $z > e$, and so

$$\sum_{2<p\leq z} p = \sum_{2<p\leq z} F(p)\log p \leq F(z)\theta^*(z).$$

Hence we shall choose z so that $F(z)\theta^*(z) = n$. If $z < 11$, then $F(z)\theta^*(z) < 11\ \log(3\cdot 5\cdot 7)/\log 11 < 22$; thus our assumption on n implies that $z \geq 11$. By Lemma 5.1A we know that $z < 2\theta^*(z)$, and so:

$$n = z\theta^*(z)/\log z < 2\theta^*(z)^2/\log 2\theta^*(z) = F(4\theta^*(z)^2).$$

However, we also have

$$F(n\log n) = (n\log n)/(\log n + \ \text{loglog}\ n) < n.$$

Since F is an increasing function this shows that $n\log n < 4\ \theta^*(z)^2$ as required. This proves the theorem. □

Exercises

5.1.3 Use the values in Table 5.2 to show that Theorem 5.1A holds when $7 \leq n \leq 26$.

TABLE 5.2.

$n =$	7	11	17	26
$\exp\sqrt{\frac{1}{4}n\log n} =$	6.33	13.04	32.14	99.68

5.1.4 Show that if h_n is the maximum order of an element in S_n, then there is an element with this order such that the lengths of its nontrivial cycles are prime powers for distinct primes.

5.1.5 Show that the maximum order of an element in A_n lies between h_n and $h_n/2$.

5.1.6 Calculate h_n for all $n \leq 30$. Can you find a general algorithm for computing h_n?

In contrast to the last theorem, the next result gives an upper bound on the order of an element in the case where the group has relatively large minimal degree.

Theorem 5.1B. *Let $G \leq Sym(\Omega)$ be a permutation group of degree n and minimal degree m. Then each element of G has order at most $n^{n/m}$.*

PROOF. Let $x \in G$ have order h. Suppose that p is a prime and that p^e ($e \geq 1$) is the largest power of p dividing h. Then $x^{h/p}$ is a product of p-cycles, and $\alpha \in \mathrm{supp}(x^{h/p})$ if and only if the cycle of x which contains α has length divisible by p^e. Thus the sum of the lengths of the cycles of x whose lengths are divisible by p^e is at least m by the hypothesis on G. This is the crucial observation which leads to the proof of the theorem.

Factor $h = q_1 \cdots q_s$ where the q_i are nontrivial powers of distinct primes, and let $h_1, \ldots, h_t$ denote the lengths of the disjoint cycles of x. For $i = 1, \ldots, s$ and $j = 1, \ldots, t$, we shall write $i \parallel j \iff q_i \mid h_j$. Then from the observation above we have $m \leq \sum_{j:i\parallel j} h_j$ for each i, and evidently we also have $\sum_{i:i\parallel j} \log q_i \leq \log h_j$ for each j. Hence

$$m \log h \leq \sum_{i=1}^{s} \log q_i \sum_{j:i\parallel j} h_j = \sum_{j=1}^{t} h_j \sum_{i:i\parallel j} \log q_i$$

and so

$$m \log h \leq \sum_{j=1}^{t} h_j \log h_j \leq \sum_{j=1}^{t} h_j \log n = n \log n$$

Thus $h \leq n^{n/m}$ as asserted. □

5.2 Subgroups of Small Index in Finite Alternating and Symmetric Groups

An early observation in the theory of permutation groups was that, apart from A_n, each proper subgroup of S_n has index at least n. When $n \neq 6$ the subgroups of index n in S_n are exactly the stabilizers of a point (S_6 also has a second conjugacy class of subgroups of index 6). More generally, for each k with $1 \leq k < \frac{n}{2}$, S_n has intransitive maximal subgroups of index $\binom{n}{k}$ isomorphic to $S_k \times S_{n-k}$. The intersections of these subgroups with A_n are subgroups of index $\binom{n}{k}$ in A_n. In fact, with a few well described exceptions, any subgroup of A_n with an index less than $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ must be intransitive and contain a substantial portion of one of the subgroups just described. This is the content of the following theorem.

Theorem 5.2A. *Let $A := Alt(\Omega)$ where $n := |\Omega| \geq 5$,, and let r be an integer with $1 \leq r \leq n/2$. Suppose that $G \leq A$ has index $|A : G| < \binom{n}{r}$. Then one of the following holds:*

(i) *for some $\Delta \subseteq \Omega$ with $|\Delta| < r$ we have $A_{(\Delta)} \leq G \leq A_{\{\Delta\}}$;*

(ii) *$n = 2m$ is even, G is imprimitive with two blocks of size m, and $|A : G| = \frac{1}{2}\binom{n}{m}$; or*

(iii) *one of six exceptional cases hold where:*

  (a) *G is imprimitive on Ω and $(n, r, |A : G|) = (6,3,15)$;*

  (b) *G is primitive on Ω and $(n, r, |A : G|, G) = (5,2,6,5{:}2)$, $(6,2,6,PSL_2(5))$, $(7,2,15,PSL_3(2))$, $(8,2,15,AGL_3(2))$, or $(9,4,120,P\Gamma L_2(8))$.*

Remark. In case (i) G contains the alternating group $A_{(\Delta)} = Alt(\Omega \setminus \Delta)$ of degree $n - r + 1$, and in case (ii) G contains two alternating groups of degree $n/2 = n - r$. In part (iii) of the theorem, the groups are listed only with the minimum r for which they satisfy the hypotheses of the theorem.

The proof uses the following elementary combinatorial lemma.

Lemma 5.2A. *Let $n > 6$ and put $m := \lfloor n/2 \rfloor$. Then:*

(i) *For each divisor t of n with $3 \leq t \leq n/2$ we have*

$$\{(n/t)!\}^t \, t! < m!(n-m)!;$$

(ii) *For each integer $t \geq 3$ and any integers $n_1, \ldots, n_t$ such that $0 < n_1 \leq \ldots \leq n_t \leq n/2$ and $\sum n_i = n$ we have*

$$\frac{n_1! \cdots n_t!}{m!(n-m)!} \leq \frac{1}{n-m} \leq \frac{1}{4}$$

PROOF. (i) Fix $t \geq 3$ and put $n = kt > 6$. Define

$$\beta(k) := \frac{m!(n-m)!}{(k!)^t t!}$$

We shall show, using induction on k, that $\beta(k) > 1$ for all $k \geq 2$ if $t > 3$ and for all $k \geq 3$ if $t = 3$. Since $t! > 2^t$ for $t > 3$, we have $\beta(2) = (t!)^2/2^t t! > 1$ for $t > 3$ and $\beta(3) = 4!5!/(3!)^3 3! > 1$ for $t = 3$. Now consider how $\beta(k)$ changes as k is increased by 1 and t is left fixed. There will be t new factors introduced in the numerator, each greater than or equal to $m + 1$, and t new factors equal to $k + 1$ introduced into the denominator. Hence for $k \geq 2$:

$$\frac{\beta(k+1)}{\beta(k)} \geq \frac{(m+1)^t}{(k+1)^t} \geq 1$$

because $k = n/t \leq n/3$. Thus induction shows that $\beta(k) > 1$ for all required values of k.

(ii) For any integers r and s greater than 0 we have $\binom{r+s}{r} \geq \binom{r+s}{1}$, and so $r!s! \leq 1!(r+s-1)!$. Using this latter inequality it is easy to see that the numerator of the expression on the left hand side of the inequality in (ii) attains its maximum value (for fixed n and t) when

$$n_1 = \ldots = n_{t-2} = 1, n_{t-1} = n - m - t + 2 \quad \text{and} \quad n_t = m.$$

Since $t \geq 3$

$$m!(n-m)!/m!(n-m-t+2)! \geq n - m \geq 4$$

and so the required inequality follows. □

PROOF OF THEOREM 5.2A. Suppose that G is a group satisfying the hypotheses of the theorem, and that case (ii) does not hold. Put $h := |A : G|$ and $m := \lfloor n/2 \rfloor$, and note that $\binom{n}{m} \geq \binom{n}{r}$ holds for $r = 0, 1, \ldots, n$.

First, if G is primitive, and $G \neq A$, then by Bochert's Theorem (Theorem 3.3B) we have $h \geq \frac{1}{2} \lfloor (n+1)/2 \rfloor !$. When $n \geq 15$ or $n = 13$, this implies that $h \geq \binom{n}{m}$ (see Exercise 5.2.1) which is contrary to hypothesis. Hence, if G is primitive, then either $n \leq 12$, $n = 14$ or $G = A$ (and so (i) holds with $\Delta = \emptyset$). An examination of the primitive groups of degrees up to 12 and of degree 14 yields the list of exceptional primitive groups given in part (iii) of the theorem (Exercise 5.2.3–5.2.6).

Now suppose that G is not primitive (and (ii) does not hold). Then we claim that either $n \leq 6$, or G is intransitive. Indeed, suppose that G is transitive, and that G has t blocks of imprimitivity of size n/t with $2 \leq t \leq n/2$. Then G is isomorphic to a subgroup of even permutations in a wreath product of order $\{(n/t)!\}^t t!$ (see Exercise 2.6.2). Thus

$$\binom{n}{m} > h \geq \frac{n!/2}{\{(n/t)!\}^t \, t!/2}.$$

If $t = 2$ (and so n is even), this inequality implies that $h = \frac{1}{2}\binom{n}{m}$ which is the case listed in (ii) of the theorem. On the other hand, if $t \geq 3$, then Lemma 5.2A (i) shows that $n \leq 6$, and an examination of Table 2.1 gives the imprimitive exception listed in (iii). In particular, we have proved that if a transitive group G of degree n has index less than $\frac{1}{2}\binom{n}{m}$ in the alternating group, then either $G = A$ (case (i)) or G is one of the exceptional groups in case (iii).

There remains the case where G is intransitive. Again we leave the case $n \leq 6$ as an exercise (Exercise 5.2.5) and assume that $n > 6$. We first show that G has an orbit of length greater than m. Suppose the contrary. If G has an orbit Γ of length exactly m, $G \leq A_{\{\Gamma\}}$, and so $|A : G| \geq |A : A_{\{\Gamma\}}| = \binom{n}{m}$ contrary to hypothesis. On the other hand, suppose the orbits of G have lengths $n_1, \ldots, n_t$ which are all less than m (so $t \geq 3$). Then using Lemma 5.2A (ii) we conclude that $|G| \leq n_1! \cdots n_t! < \frac{1}{4}m!(n-m)!$, which again contradicts the condition that $|A : G| < \binom{n}{m}$. Thus G has an orbit Γ, say, of length $s > m \geq 3$.

Define $\Delta := \Omega \setminus \Gamma$ and $H := G_{(\Delta)} \leq A_{(\Delta)} = Alt(\Gamma)$; our object is to show that $H = A_{(\Delta)}$. Put $h' := |A_{(\Delta)} : H|$. Since $|A : G|\,|G : H| = |A : A_{(\Delta)}|\,|A_{(\Delta)} : H|$, and $G/H \cong G^{\Delta} \leq Sym(\Delta)$, we have $h(n-s)! \geq (n!/s!)h'$. Thus, if we put $t := \lfloor s/2 \rfloor$, then the hypothesis on h shows that

$$h' \leq \frac{(n-s)!s!}{n!}h < \frac{(n-s)!s!}{(n-m)!m!} = \frac{(n-s)!t!(s-t)!}{(n-m)!m!}\binom{s}{t}.$$

Hence Lemma 5.2A (ii) yields

$$h' \leq \frac{1}{n-m}\binom{s}{t} \leq \frac{1}{4}\binom{s}{t}.$$

Now induction applied to H acting on Γ shows that one of three things can happen: (i) there exists an H-invariant subset $\Sigma \subseteq \Gamma$ with $|\Sigma| < s/2$ such that $A_{(\Delta\cup\Sigma)} \leq H$; (ii) $h' = \frac{1}{2}\binom{s}{t}$; or (iii) $s \leq 9$, and H^{Γ} is one of the exceptional groups listed in the theorem. The second of these possibilities cannot hold because of the bound on h' given above. Also, since $n - m \geq \lfloor (n+1)/2 \rfloor \geq \lfloor (s+2)/2 \rfloor$, the bounds for h' given above also show that h' is at most 3, 5, 8, 14 and 25 for $s = 5, 6, 7, 8$ and 9, respectively. Thus $H^{\Gamma}$is not one of the exceptional cases in (iii). Therefore we conclude that (i) holds, and so $H^{\Gamma\setminus\Sigma} \geq A^{\Gamma\setminus\Sigma}$; and since $|\Gamma \setminus \Sigma| > s/2 \geq 2$, this shows that $\Gamma \setminus \Sigma$ is an orbit of H. However, G acts transitively on Γ, and $H = G_{(\Delta)} \triangleleft G$, so the lengths of the orbits of H on Γ divide $s = |\Gamma|$ (Theorem 1.6B). Therefore $\Sigma = \emptyset$, and Γ itself is an orbit for H. Thus $A_{(\Delta)} = H \leq G \leq A_{\{\Delta\}}$ and the proof of the theorem is complete. □

Corollary 5.2A. *Let Ω be a finite set of size $n > 9$, and s be an integer satisfying $n/2 < s < n$. If $G \leq A := Alt(\Omega)$ has index $|A : G| <$*

min $\left\{\binom{n}{s}, \frac{1}{2}\binom{n}{\lfloor n/2 \rfloor}\right\}$ *then G has a unique orbit Γ such that $|\Gamma| \geq n/2$ and $G_{\{\Gamma\}}$ induces either the alternating or symmetric group on Γ.*

PROOF. The hypotheses of the Theorem 5.2A hold and the cases (ii) and (iii) have been excluded. Thus G satisfies (i) with $r = n - s$. We take $\Gamma = \Omega \setminus \Delta$; then $|\Gamma| > s + 1$ and $G_{\{\Gamma\}}$ contains $A_{(\Delta)}$ which acts as the alternating group on Γ. □

Exercises

5.2.1 Show that $\frac{1}{2}\ \lfloor (n+1)/2 \rfloor! > \binom{n}{\lfloor n/2 \rfloor}$ for all $n \geq 15$ and for $n = 13$.

5.2.2 Show that the intransitive subgroups $S_k \times S_{n-k} < S_n$ are maximal for $1 \leq k < \lfloor \frac{n}{2} \rfloor$.

5.2.3 Use the list of groups of degree 7 given in Table 2.1 to show that the only primitive groups of degree 8 or 9 which are exceptional in Theorems 5.2A or 5.2B are those listed.

5.2.4 (Continuation) Using Theorems 3.3B and 3.3E show that there is no exceptional primitive group of degree 14.

5.2.5 (Continuation) Show that there is no exceptional primitive group of degree 10. [*Hint:* It is enough to show that there is no proper primitive group $G \leq Sym(\Omega)$ of degree 10 and order $g \geq \frac{1}{2}(5!)^2 = 7200$. Suppose the contrary. Note that Theorem 3.3E implies that neither 7 nor 5^2 divides g. Since $7 \mid 210 = \left|\Omega^{\{4\}}\right|$, G does not act transitively on $\Omega^{\{4\}}$, and so there exists $\Delta \in \Omega^{\{4\}}$ such that $h := \left|G : G_{\{\Delta\}}\right| \leq 210/2$. Since $h \mid g$, this implies that $h \leq 96$, and so $H := G_{\{\Delta\}}$ has order at least $7200/96 = 75$. Put $\Gamma := \Omega \setminus \Delta$. Since G has no nontrivial element whose support has size ≤ 4 (see Sect. 3.3), $H_{(\Gamma)} = 1$, and so $H \cong H^\Gamma$. Now Table 2.1 shows that $H^\Gamma \cong PGL_2(5)$, A_6 or S_6; and in each case H^Γ contains a 5-cycle. If $x \in H$ is chosen so that x^Γ is a 5-cycle, then some power of x is a 5-cycle in H because 5 does not divide the order of x^Δ. This contradicts Theorem 3.3E.]

5.2.6 (Continuation) Give similar proofs to show that there are no exceptional primitive groups of degree 11 or 12.

A result similar to Theorem 5.2A holds for the finite symmetric groups. If G is a subgroup of S_n for some n and $|S_n : G| < \binom{n}{r}$ for some $r \leq n/2$ then $|A_n : G \cap A_n| < \binom{n}{r}$ and Theorem 5.2A applies to $G \cap A_n$. However some new exceptional cases arise. We leave the proof as an exercise.

Theorem 5.2B. *Let $S := Sym(\Omega)$ and $A := Alt(\Omega)$ where $n := |\Omega| \geq 5$, and let r be an integer with $1 \leq r \leq n/2$. Suppose that $G \leq S$ has index $|S : G| < \binom{n}{r}$. Then one of the following holds:*

(i) *for some $\Delta \subseteq \Omega$ with $|\Delta| < r$ we have $A_{(\Delta)} \leq G \leq S_{\{\Delta\}}$;*

(ii) *$n = 2m$ is even, G is imprimitive with two blocks of size m, and $|S : G| = \frac{1}{2}\binom{n}{m}$; or*

(iii) *one of six exceptional cases hold where:*

(a) *G is imprimitive with blocks of size 2 on Ω and* $(n, r, |S : G|) =$ *(6,3,15) ;*
(b) *G is primitive on Ω and* $(n, r, |S : G|, G) =$ *(5,2,6,5:4), (6,2,6,$PGL_2(5)$), (6,2,12,$PSL_2(5)$), (7,3,30,$PSL_3(2)$), or (8,3,30,$AGL_3(2)$).*

Remark. In part (iii) of the theorem, the groups are listed only with the minimum r for which they satisfy the hypotheses of the theorem.

Exercise

5.2.7 Starting with the remarks preceeding Theorem 5.2B, complete the proof of the theorem.
5.2.8 Show that each maximal subgroup of the symmetric group $S := Sym(\Omega)$ of finite degree n is either primitive or one of the following:
(i) (intransitive) the set stabilizer $S_{\{\Delta\}}$for some subset $\Delta \subseteq \Omega$ with $1 \leq |\Delta| < n/2$; or
(ii) (imprimitive) the subgroup $S[\Pi]$ consisting of all permutations which preserve a partition $\Pi = \{\Delta_1, \ldots, \Delta_m\}$ of Ω into parts of size n/m with $1 < m < n$.

Conversely, show that each of the subgroups in (i) and (ii) is maximal in S. (The case where S is an infinite symmetric group is much more complicated; some information is given in Chapter 8.)
5.2.9 (Continuation) State and prove the analogous result for the alternating group.

5.3 The Order of a Simply Primitive Group

Among the main theorems of this chapter are bounds due to Babai (1981) and (1982) (and refined by L. Pyber) on the order of a proper primitive group. We deal separately with the case where the group is 2-transitive and where it is *simply primitive* (that is, primitive, but not 2-transitive). In this section we focus on the simply primitive case.

The following notation will be fixed for the rest of this section. Let $G \leq Sym(\Omega)$ be a transitive group of finite degree n. Let $\Delta_1, \ldots, \Delta_r$ be the orbitals of G where Δ_1 is the diagonal orbital, and Δ_i^* denotes the orbital paired with the orbital Δ_i (see Section 3.2).

Since G is transitive on Ω, the length n_i of the suborbit $\Delta_i(\alpha)$ is independent of the choice of $\alpha \in \Omega$. We shall assume that the orbitals are ordered so that $1 = n_1 \leq n_2 \leq \ldots \leq n_r$. If α, β and γ lie in Ω, then we shall say that γ *discriminates* between α and β if (α, γ) and (β, γ) lie in different orbitals; in this case we shall use the notation $(\alpha, \gamma) \# (\beta, \gamma)$. We shall write

$$\Psi_{\alpha\beta} := \{\gamma \in \Omega \mid (\alpha, \gamma) \# (\beta, \gamma)\}$$

and call this the *discriminating set* for α and β. Clearly $\Psi_{\alpha\beta} = \Psi_{\beta\alpha}$, and $\Psi_{\alpha\alpha} = \emptyset$. If $\alpha \neq \beta$ then $\Psi_{\alpha\beta}$ contains at least two elements, namely α and β.

Exercises

5.3.1 If $\Sigma \subseteq \Omega$ and $\Sigma \cap \Psi_{\alpha\beta} \neq \emptyset$ for all pairs of distinct points α and β, show that Σ is a base for G.
5.3.2 Show that the value of $|\Psi_{\alpha\beta}|$ only depends on the orbital Δ_i to which (α, β) belongs.
5.3.3 If G is regular of degree n, show that each discriminating set $\Psi_{\alpha\beta}$ with $\alpha \neq \beta$ has size n.

We define $d(G)$ to be the minimum of $|\Psi_{\alpha\beta}|$ taken over all pairs of distinct points α and β. If G is 2-transitive ($r = 2$), then $|\Psi_{\alpha\beta}| = 2$ for all pairs of distinct α and β, and hence $d(G) = 2$; the discriminating sets are not very interesting in this case. If G is regular, then $d(G) = n$. Our first result shows how the invariant $d(G)$ is related to the minimal degree and the size of a base for G.

Lemma 5.3A. *Let G be a transitive group of degree n, and put $d := d(G)$. Then:*
(i) *The minimal degree of G is at least d; and*
(ii) *G has a base of size at most $n(2\log n - \log 2)/d$.*

PROOF. (i) Let $x \neq 1$ and choose $\alpha, \beta \in \Omega$ such that $\alpha^x = \beta \neq \alpha$. Then no $\gamma \in \Psi_{\alpha\beta}$ is fixed by x, and so $|\mathrm{supp}(x)| \geq |\Psi_{\alpha\beta}| \geq d$.

(ii) It is enough to show that if s is an integer such that $0 < s \leq n$ and no s-subset of Ω is a base for G, then $s < n(2\log n - \log 2)/d$. Consider the set $\Omega^{\{s\}}$ of all subsets of size s, and for each ordered pair (α, β) define $\chi_{\alpha\beta}$ on $\Omega^{\{s\}}$ by putting $\chi_{\alpha\beta}(\Sigma) := 1$ if $\Sigma \cap \Psi_{\alpha\beta} = \emptyset$, and $\chi_{\alpha\beta}(\Sigma) := 0$ otherwise.

Now define $m := \sum \chi_{\alpha\beta}(\Sigma)$ where the sum is over all $\Sigma \in \Omega^{\{s\}}$ and all $(\alpha, \beta) \in \Omega^{(2)}$. We shall estimate m in two different ways under the assumption that no element of $\Omega^{\{s\}}$ is a base for G.

First, if we sum $\chi_{\alpha\beta}(\Sigma)$ over $\Sigma \in \Omega^{\{s\}}$ for a fixed pair (α, β), we see that this sum is equal to the number of ways of choosing an s-subset from $\Omega \setminus \Psi_{\alpha\beta}$. Since $|\Psi_{\alpha\beta}| \geq d$ whenever $\alpha \neq \beta$, this shows that

$$m \leq n(n-1)\binom{n-d}{s}.$$

Second, we fix Σ and sum over $(\alpha, \beta) \in \Omega^{(2)}$. Since Σ is not a base for G by hypothesis, there is at least one pair (α, β) such that $\Sigma \cap \Psi_{\alpha\beta} = \emptyset$ (see Exercise 5.3.1 above). For this pair we have $\chi_{\alpha\beta}(\Sigma) = \chi_{\beta\alpha}(\Sigma) = 1$. Since this is true for each $\Sigma \in \Omega^{\{s\}}$ we have

$$m \geq 2\left|\Omega^{\{s\}}\right| = 2\binom{n}{s}.$$

Combining these two inequalities for m we get

$$n(n-1)\prod_{k=n-s+1}^{n}\left(1-\frac{d}{k}\right) = \frac{n(n-1)\binom{n-d}{s}}{\binom{n}{s}} \geq 2.$$

Hence $n^2(1-d/n)^s > 2$, and so

$$2\log n - \frac{sd}{n} > 2\log n + s\log\left(1-\frac{d}{n}\right) > \log 2.$$

Thus, if there is no base of size s for G, then $s < n(2\log n - \log 2)/d$. This proves (ii). □

We now turn to estimating $d(G)$ for a primitive group G of rank $r > 2$. This will lead to the main theorem on the size of a base and the minimal degree of a simply primitive permutation group. Before stating the lemma we introduce some further notation. Let $\mathcal{G}_i = \text{Graph}(\Delta_i)$ be the digraph for the orbital Δ_i, and recall that, for a finite primitive group G, the graph $\mathcal{G}_i$ is strongly connected when $i > 1$ (see Lemma 3.2A). We also define $\overline{\mathcal{G}_i}$ to be the (nondirected) graph on the vertex set Ω with an edge between α and $\beta \iff$ either (α,β) or (β,α) lies in Δ_i. When G is primitive and $i > 1$, the graph $\overline{\mathcal{G}_i}$ is connected, and we can define diam(i) to be the diameter of $\overline{\mathcal{G}_i}$ (that is, the greatest distance between any pair of vertices in $\overline{\mathcal{G}_i}$). We shall use d_i to denote $|\Psi_{\alpha\beta}|$ when $(\alpha,\beta) \in \Delta_i$; by Exercise 5.3.2 this is independent of the choice of (α,β).

Lemma 5.3B. *Suppose that G is a finite primitive group of degree n and rank $r > 2$. Then $d(G) > \sqrt{n}/2$.*

PROOF. We use the notation established above. We first show that, for all $\alpha, \beta \in \Omega$ and each $i > 1$, there exists at least one $\gamma \in \Omega$ such that $(\beta,\gamma) \in \Delta_i$ and $(\alpha,\beta) \# (\alpha,\gamma)$. Indeed, let Γ be the orbit of β under G_α. Since G is a finite primitive group and $i > 1$, the graph $\mathcal{G}_i$ is strongly connected and so there is a directed path in $\mathcal{G}_i$ from any point in Γ to a point not in Γ. Somewhere along such a path there will exist consecutive vertices, say β' and γ', such that $\beta' \in \Gamma$, $\gamma' \notin \Gamma$ and $(\beta',\gamma') \in \Delta_i$. Since Γ is a G_α-orbit, there exists $x \in G_\alpha$ such that $\beta = (\beta')^x$. If we define $\gamma := (\gamma')^x$, then $(\beta,\gamma) \in \Delta_i$ and $(\alpha,\beta) \# (\alpha,\gamma)$ because $(\alpha,\beta') \# (\alpha,\gamma')$, which gives what we required.

We shall now prove that

$$(5.1) \qquad n_i d_i > n \quad \text{for all } i > 1\ .$$

Indeed, count the number m of triples (α,β,γ) with $(\beta,\gamma) \in \Delta_i$ and $(\alpha,\beta) \# (\alpha,\gamma)$ in two ways. First, summing over $(\beta,\gamma) \in \Delta_i$ we get $m = |\Delta_i|\, d_i = n_i n d_i$. Second, summing over $(\alpha,\beta) \in \Omega \times \Omega$, and using the result established above, gives $m \geq n^2$. Now (5.1) follows.

We next show that

(5.2) if $(\alpha, \beta) \in \Delta_j$, and α and β are distance t in $\overline{\mathcal{G}_i}$, then $d_j \leq td_i$.

To show this, consider the sequence of vertices $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_t = \beta$ on a path from α to β of length t in $\overline{\mathcal{G}_i}$. If $\gamma \in \Omega$, then $(\alpha, \gamma) \# (\beta, \gamma)$ implies $(\alpha_k, \gamma) \# (\alpha_{k+1}, \gamma)$ for some k with $0 \leq k < t$. Hence

$$\Psi_{\alpha\beta} \subseteq \bigcup_{k=0}^{t-1} \Psi_{\alpha_k \alpha_{k+1}}.$$

Thus $d_j \leq td_i$ and (5.2) is proved.

As our last preliminary result we show that

(5.3) there exists $k > 1$ such that $d_k > \sqrt{n}$.

Suppose the contrary. Then (5.1) shows that $n_i > n/d_i \geq \sqrt{n}$ for all $i > 1$. Now for each $\gamma \in \Omega$, the number of pairs $(\alpha, \beta) \in \Omega \times \Omega$ such that $(\alpha, \gamma) \# (\beta, \gamma)$ is equal to

$$m := n^2 - \sum_{i=1}^{r} n_i^2 = 2 \sum_{i<j} n_i n_j.$$

Thus

$$m = \sum_{i=1}^{r} n_i(n - n_i) > \sum_{i=2}^{r} \sqrt{n}(n - n_i) > (r-2)n\sqrt{n} \geq n\sqrt{n}.$$

Since there is a total of nm points lying in the sets $\Psi_{\alpha\beta}$ $((\alpha, \beta) \in \Omega^{(2)})$, we conclude that for some (α, β) we have $\left|\Psi_{\alpha\beta}\right| \geq nm/n(n-1) > \sqrt{n}$. This contradicts our assumption that all $d_i < \sqrt{n}$, and (5.3) is proved.

Finally, to prove the lemma we must show that $d_i > \sqrt{n}/2$ for all $i > 1$. In the case that $\operatorname{diam}(i) = 2$, this follows at once from (5.3) and (5.2). On the other hand, if $\operatorname{diam}(i) \geq 3$, then choose α and β at distance 3 in $\overline{\mathcal{G}_i}$. Then, for each $\gamma \in \Omega$ lying at distance exactly 1 from α or β, exactly one of (α, γ) and (β, γ) lies in $\Delta_i \cup \Delta_i^*$, and so $\gamma \in \Psi_{\alpha\beta}$. Thus, if $(\alpha, \beta) \in \Delta_j$, say, then $d_j \geq 2n_i$. Now applying (5.2) and (5.1) we obtain $d_i^2 \geq d_i d_j/3 \geq 2d_i n_i/3 > 2n/3$, and so $d_i > \sqrt{n}/2$ in this case as well. □

Combining these results gives the desired bound on the index of a simply primitive permutation group.

Theorem 5.3A. *Let G be a permutation group of degree n which is primitive but not 2-transitive. Then*

(i) *The minimal degree of G is greater than $\sqrt{n}/2$;*

(ii) *G has a base Σ with $|\Sigma| < 4\sqrt{n} \log n$;*

(iii) $|G| < \exp(4\sqrt{n}(\log n)^2)$.

PROOF. (i) Immediate from the last two lemmas.

(ii) The last two lemmas show that G has a base Σ with $|\Sigma| < n(2\log n - \log 2)/(\sqrt{n}/2) < 4\sqrt{n}\log n$.

(iii) For any base Σ of G we have

$$|G| \leq n(n-1)\cdots(n-|\Sigma|+1) \leq \exp(|\Sigma|\log n)$$

and so (iii) follows from (ii). □

Exercise

5.3.4 Consider the action of $Sym(\Omega)$ on $\Omega^{\{2\}}$ where $|\Omega| = m > 4$. Show that the image G of this action is a primitive group of degree $n := \binom{m}{2}$ which is not 2-transitive, that G has minimal degree $< 2\sqrt{2n}$, that the smallest base of G has size greater than

$$\frac{1}{2}\left\{\sqrt{n/2} - 1/\log n\right\}$$

and that

$$|G| \geq \exp(\sqrt{2n}\log\sqrt{2n} - \sqrt{2n}).$$

5.4 The Minimal Degree of a 2-transitive Group

We have already seen that a finite 2-transitive group of degree n which does not contain the alternating group has minimal degree at least $\sqrt{n-1}+1$ (Theorem 3.3D). Our object in the present section is to present better bounds due to Bochert (1897).

Theorem 5.4A. *Let G be a 2-transitive group of degree n which does not contain the alternating group, and suppose that G has minimal degree m. Then we have the following lower bounds for m:*
(i) $m > \sqrt{n-1}+1 \geq \sqrt{n}$ *for all n;*
(ii) $m \geq n/8$ *for all n;*
(iii) $m \geq n/4$ *for all $n > 216$.*

Part (i) follows from the comment above. The proof of parts (ii) and (iii) will proceed from a series of lemmas. In these lemmas we shall assume that $G \leq Sym(\Omega)$ is 2-transitive with $|\Omega| = n$, and that G has minimal degree $m > 3$ since a 2-transitive group with minimal degree 2 or 3 is the symmetric or the alternating group, respectively (see Theorem 3.3A). Fix an element $u \in G$ with support Γ of size m, and define

$$T := \{x \in G \mid [u, x^{-1}ux] \neq 1\}$$

where, as usual, $[y,z] := y^{-1}z^{-1}yz$. Put $t := |T|$ and $g := |G|$.

Lemma 5.4A. *With the notation above:*
(i) $|\Gamma \cap \Gamma^x| \geq m/3$ *for all $x \in T$;*

(ii) *if* $x^{-1}ux \notin G_{\{\Gamma\}}$ *then* $x \in T$*;*
(iii) $t/g \geq 2m(n-m)/n(n-1)$.

PROOF. (i) Since $\Delta := \Gamma \cap \Gamma^x = \mathrm{supp}(u) \cap \mathrm{supp}(x^{-1}ux)$, Exercise 1.6.7 shows that

$$\mathrm{supp}([u, x^{-1}ux]) \subseteq \Delta \cup \Delta^u \cup \Delta^{x^{-1}ux}.$$

Since all the sets on the right hand side have the same size, $[u, x^{-1}ux] \neq 1$ implies that $|\Delta| \geq m/3$ by the definition of m.

(ii) If $x \notin T$, then $x^{-1}ux$ centralizes u, and hence the support Γ of u is mapped into itself by $x^{-1}ux$.

(iii) Fix $\alpha \in \Gamma$ and put $\beta := \alpha^u \in \Gamma$. Since G is 2-transitive, there are exactly $g/n(n-1)$ elements in G which map $(\alpha, \beta) \in \Omega^{(2)}$ onto any specified pair in $\Omega^{(2)}$. In particular, there is a total of $2gm(n-m)/n(n-1)$ elements $x \in G$ such that exactly one of the points α^x, β^x lies in Γ. Since $(\alpha^x)^{x^{-1}ux} = \beta^x$, it follows from (ii) that each such x lies in T, and so we get the required lower bound on t/g. □

Lemma 5.4B. *For each* $x \in G$ *we put* $c_x := |\Gamma \cap \Gamma^x|$*. Then:*
(i) $\frac{1}{g}\sum_{x \in G} c_x = \frac{m^2}{n}$ *(the "mean value" of* c_x*);*
(ii) $\frac{1}{g}\sum_{x \in G} c_x(c_x - 1) = \frac{m^2(m-1)^2}{n(n-1)}$;
(iii) $\frac{1}{g}\sum_{x \in G}(c_x - \frac{m^2}{n})^2 = \frac{m^2(n-m)^2}{n^2(n-1)}$ *(the "variance" of* c_x*).*

PROOF. (i) Clearly, $\sum c_x = |\Lambda_1|$ where

$$\Lambda_1 := \{(\alpha, x) \in \Gamma \times G \mid \alpha^x \in \Gamma\}.$$

Transitivity of G shows that for fixed $\alpha, \beta \in \Gamma$, there are exactly $|G_\alpha| = g/n$ elements of $x \in G$ such that $\alpha^x = \beta$. Since $|\Gamma| = m$, this shows that $|\Lambda_1| = m^2 g/n$ and so (i) follows.

(ii) Similarly, $\sum c_x(c_x - 1) = |\Lambda_2|$ where

$$\Lambda_2 := \{(\alpha, \beta, x) \in \Gamma \times \Gamma \times G \mid \alpha^x, \beta^x \in \Gamma \text{ and } \alpha \neq \beta\}.$$

Since G acts transitively on $\Omega^{(2)}$, for any two pairs $(\alpha, \beta), (\gamma, \delta) \in \Gamma^{(2)}$ there exist exactly $|G_{\alpha\beta}| = g/n(n-1)$ elements $x \in G$ such that $(\alpha, \beta)^x = (\gamma, \delta)$. Because $|\Gamma^{(2)}| = m(m-1)$, this shows that $|\Lambda_2| = m^2(m-1)^2 g/n(n-1)$ as required.

(iii) Put $c := m^2/n$. Then using (i) and (ii) we have:

$$\begin{aligned}\sum (c_x - c)^2 &= \sum c_x^2 - gc^2 \\ &= g\left\{\frac{m^2(m-1)^2}{n(n-1)} + \frac{m^2}{n} - \frac{m^4}{n^2}\right\} \\ &= \frac{gm^2(n-m)^2}{n^2(n-1)}\end{aligned}$$

and the lemma is proved. □

PROOF OF THEOREM 5.4A. It remains to establish parts (ii) and (iii). We shall use the notation just introduced. If $m \geq n/3$ then there is nothing to prove, so suppose that $m < n/3$. By Lemma 5.4A we know that when $x \in T$ then $c_x \geq m/3$ and so $c_x - m^2/n \geq m/3 - m^2/n \geq 0$. Thus by Lemma 5.4B (iii)

$$\frac{m^2(n-m)^2}{n^2(n-1)} \geq \frac{1}{g}\sum_{x \in T}\left(c_x - \frac{m^2}{n}\right)^2 \geq \frac{t}{g}\left(\frac{m}{3} - \frac{m^2}{n}\right)^2.$$

Then using Lemma 5.4A (iii) and simplifying we get

$$n(n-m) \geq 2m\left(\frac{n}{3} - m\right)^2. \tag{5.4}$$

Now substitute $m = \lambda n/3$, and note that $\lambda > 3/\sqrt{n}$ by part (i) of the theorem. The inequality (5.4) becomes

$$n \leq f(\lambda) \quad \text{with} \quad \frac{3}{\sqrt{n}} < \lambda < 1 \tag{5.5}$$

where

$$f(\mu) := \frac{9(3-\mu)}{2\mu(1-\mu)^2}.$$

Elementary calculus shows that f has a unique minimum value in the interval (0,1) at the point $\mu_0 := (9-\sqrt{57})/4 = 0.3625\ldots$. We claim that $\lambda > \mu_0$ for all n. In fact, (i) implies that, for all $n \leq 78$:

$$\lambda = \frac{3m}{n} \geq \frac{3(\sqrt{n-1}+1)}{n} \geq \frac{3(\sqrt{77}+1)}{78} = 0.3759\ldots > 3/8 > \mu_0$$

so consider the case where $n > 78$. We can rewrite inequality (5.5) as

$$2n\lambda(1-\lambda) \leq \frac{9(3-\lambda)}{(1-\lambda)}$$

and note that the two functions $\mu \mapsto \mu(1-\mu)$ and $\mu \mapsto (3-\mu)/(1-\mu)$ are both increasing on the interval $[3/\sqrt{n}, \mu_0]$. Hence $\lambda \leq \mu_0$ implies

$$2n\left(\frac{3}{\sqrt{n}}\right)\left(1 - \frac{3}{\sqrt{n}}\right) \leq \frac{9(3-\mu_0)}{(1-\mu_0)}.$$

This shows that $6\sqrt{n} - 18 \leq 37.237\ldots$ and so $n \leq 84$. Thus the only possible cases for which $\lambda \leq \mu_0$ can occur satisfy $79 \leq n \leq 84$. However (i) shows that if $79 \leq n \leq 81$, then $m > 9$ and so $\lambda = 3m/n \geq 30/81 = 0.3703\ldots > \mu_0$. Similarly, if $82 \leq n \leq 84$, then $m > 10$ and so $\lambda \geq 33/84 = 0.3928\ldots > \mu_0$. This proves that $\lambda > \mu_0$ in all cases.

The proofs of (ii) and (iii) now follow easily. To prove (ii), we must show that $\lambda \geq 3/8$ for all n. However, since the function f in the inequality (5.5) is increasing on $(\mu_0, 1)$, and since $\lambda > \mu_0$ from above, it follows from

inequality (5.5) that $\lambda < 3/8$ implies that $n < f(3/8) = 80.64$. We saw above that $\lambda > 3/8$ for all $n \leq 78$, and so the only remaining cases to consider are $n = 79$ and 80. But (i) again shows that $m > 9$ for all $n \geq 66$, and so $\lambda = 3m/n \geq 30/80 = 3/8$ for $n = 79$ or 80. This proves (ii).

The proof of (iii) is similar. We have to show that $\lambda \geq 3/4$ for all $n > 216$, and this follows from inequality (5.5) since $f(3/4) = 216$. □

Exercises

5.4.1 Prove, under the hypothesis of Theorem 5.4A, that for each $\theta > 1$ there exists n_0 such that $m > n/3 - \theta\sqrt{n}$ whenever $n \geq n_0$.

5.4.2 Show that there exists a constant $c_0 > 0$ such that, if G is a proper 2-transitive permutation group of degree n, then every element of G has order $< c_0 n^3$. [*Hint:* Use Theorem 5.1B.]

5.4.3 Show that there exists a constant $c_1 > 0$ such that, if G is a proper 2-transitive permutation group of degree n, then the largest k for which A_k is isomorphic to a section of G is bounded by $k < c_1(\log n)^2/(\log\log n)$. In particular, if G is k-transitive of degree n then k must satisfy this inequality. [*Hint:* Use Theorem 5.1A and the preceding exercise. A stronger result will be proved in Sect. 5.5.]

EXAMPLE 5.4.1. The affine group $AGL_d(q)$ acts as a permutation group on the affine space of dimension d over a field of q elements. The fixed points of each $x \in AGL_d(q)$ form an affine subspace. Thus the maximum number of fixed points of a nonidentity element of $AGL_d(q)$ is q^{d-1}. Since there are nonidentity transformations fixing a hyperplane pointwise, the minimal degree of $AGL_d(q)$ is $m = q^d - q^{d-1} = (1 - \frac{1}{q})n$ where $n := q^d$ is the degree. In particular if $q = 2$ then $m = n/2$. Some transitive subgroups of $GL_d(q)$, such as the symplectic groups $Sp_d(q)$, also contain elements fixing a hyperplane pointwise and so give further examples of 2-transitive groups with $m = n/2$.

EXAMPLE 5.4.2. The groups $A\Gamma L_d(q)$ and $P\Gamma L_d(q)$ may contain permutations, induced by field automorphisms, with fixed point sets that are not subspaces over $\mathbb{F}_q$ but rather subgeometries defined over a subfield. Usually these fixed point sets are smaller than a hyperplane, but there are interesting exceptional cases. For example, the group $PGL_2(q)$ is sharply 3-transitive of degree $q+1$ and so has minimum degree $q-1$. If $q = p^{ab}$ where p is prime, then there is a permutation in $P\Gamma L_2(q)$ fixing $p^a + 1$ points. The group $PGL_3(4)$ has degree 21 in its action on the projective plane $PG_2(4)$; the maximum number of fixed points of a nontrivial element is 5 but the field automorphism induces a permutation that fixes a Fano subplane of 7 points. These permutations will resurface in Chap. 6.

EXAMPLE 5.4.3. The symplectic groups $Sp_{2d}(2)$, for $d \geq 2$, have two distinct 2-transitive permutation representations with degrees $n^- = 2 \cdot 4^{d-1} - 2^{d-1}$ and $n^+ = 2 \cdot 4^{d-1} + 2^{d-1}$ respectively (see Sect. 7.7). In each case there are involutions that fix 4^{d-1} points and the minimal degrees of the two representations of $Sp_{2d}(2)$ are $m^- = 4^{d-1} - 2^{d-1}$ and $m^+ = 4^{d-1} + 2^{d-1}$. Since

$$\frac{m^\pm}{n^\pm} = \frac{1}{2}\left(1 \pm \frac{1}{2^d \pm 1}\right)$$

the minimal degree is slightly less than half the points in the action of degree n^- and slightly more than half the points in the other case.

5.5 The Alternating Group as a Section of a Permutation Group

The theorems of the present section give further lower bounds for the minimal degree of a permutation group. Theorem 5.5A shows that any permutation group which has a section isomorphic to A_k for a large value of k must have a relatively large degree or a small minimal degree. Theorem 5.5B applies this result to 2-transitive groups. The argument of this section originated with work of Wielandt (1934) on k-transitive groups. Since a k-transitive group has a section isomorphic to A_k, Theorem 5.5B shows that a proper k-transitive group of degree n has $k < 6 \log n$. (In fact the classification of finite simple groups shows that $k < 6$; see Sect. 7.3). In Theorem 5.6B, we will use Theorem 5.5B to bound the order of a finite multiply transitive group.

We begin by looking at a special class of groups which have specified sections. Let G and U be arbitrary groups. We say that G is a *preimage* of U with kernel K, if $K \lhd G$ and $G/K \cong U$; and say that G is a *minimal preimage* of U if G is a preimage but no proper subgroup of G is a preimage of U.

Lemma 5.5A. *If U and G are finite groups, and G is a minimal preimage of U with kernel K then the following hold.*

(i) *If $H \leq G$ and $HK = G$, then $H = G$.*
(ii) *K is nilpotent.*
(iii) *If U is simple, then each proper normal subgroup M of G is contained in K, and G/M is also a minimal preimage of U.*
(iv) *Suppose $G \leq H$ and $N \lhd H$. If U is simple and H/N has no section isomorphic to U, then $G \leq N$.*

PROOF. (i) Since $H/(H \cap K) \cong G/K \cong U$, the minimality of G shows that $H = G$.

(ii) A finite group is nilpotent if and only if each of its Sylow subgroups is normal. Let P be a Sylow subgroup of K. Then the Frattini argument (see Exercise 1.4.14) shows that $G = N_G(P)K$, and so $G = N_G(P)$ by (i). Hence $P \lhd K$, and the result follows.

(iii) Suppose that $M \lhd G$ and M is not contained in K. Since $U \cong G/K$ is simple, MK/K must equal G/K, and so $M = G$ by (i). This proves the first statement, and the second follows easily.

(iv) If G is not contained in N, then $G/(G \cap N) \cong GN/N$ is a preimage of U by (iii) contrary to the hypothesis on H/N. □

In the following lemma we use the notation $\lambda(k)$ to denote the minimum positive integer d such that for some field F the group $GL_d(F)$ has a finite subgroup with A_k as a quotient. Using methods concerned with linear groups, we shall show in Sect. 5.7 that $(2k-4)/3 \le \lambda(k) \le k-1$. In anticipation, we use these bounds in the proofs below.

Lemma 5.5B. *Let $t \ge 5$ and consider a group H with a subgroup M which is a minimal preimage of A_t. Suppose that H acts on a set Ω such that Ω is an orbit for some solvable normal subgroup K of H. If $|\Omega| < 2^{\lambda(t)}$, then M lies in the kernel of this action.*

PROOF. First consider the special case where $|\Omega| > 1$ and H acts primitively on Ω. Let $\overline{H}$ and $\overline{K}$ denote the images of H and K, respectively, in this action, and let N denote the kernel of the action. Since K acts transitively on Ω, the primitive group $\overline{H} \le Sym(\Omega)$ has a nontrivial solvable normal subgroup $\overline{K}$. Thus, by Corollary 4.3B and Theorem 4.6A, $\mathrm{soc}(\overline{H})$ is a regular elementary abelian p-subgroup for some prime p, $|\Omega| = p^d$ for some $d \ge 1$, and each point stabilizer $\overline{H}_\alpha$ is isomorphic to a subgroup of $GL_d(p)$. Since $\overline{H} = \overline{H}_\alpha \overline{K}$, we have a normal series $H \rhd KN \rhd N \rhd 1$ where H/KN is isomorphic to a section of $GL(d,p)$ and KN/N is solvable. However, $2^d \le p^d = |\Omega| < 2^{\lambda(t)}$ by hypothesis, so by the definition of $\lambda(t)$ there is no section of $GL_d(p)$ which is isomorphic to A_t. Hence $M \le N$ by Lemma 5.5A (iv). This proves the result in the case where H acts primitively.

Now consider the general case. The result is trivial if $|\Omega| = 1$, so we shall assume $|\Omega| > 1$ and proceed by induction on $|\Omega|$. Choose $\Sigma = \{\Delta_1, \ldots, \Delta_m\}$ as a system of minimal blocks for H $(m \ge 1)$. Since K acts transitively on Σ and $|\Sigma| < |\Omega|$, induction shows that M lies in the kernel of the action of H on Σ; hence $M \le H_i := H_{\{\Delta_i\}}$ for each i. Consider a fixed i, and choose $\alpha \in \Delta_i$. Then $H = H_\alpha K$ by the transitivity of K, and $H_\alpha \le H_i$ because Δ_i is a block, so $H_i = H_\alpha(K \cap H_i)$. Now H_i acts primitively on Δ_i because Δ_i is a minimal block (see Exercise 1.5.10), H_i has a solvable normal subgroup $K \cap H_i$ acting transitively on Δ_i, and $M \le H_i$. Therefore, applying the special case proved above, we conclude that M lies in the kernel of this action, namely, $M \le H_{(\Delta_i)}$. Since this is

true for each i, we have shown that M fixes every point in Ω and so lies in the kernel of the action on Ω as asserted. □

The next lemma gives a crucial step in the proof of our main theorem.

Lemma 5.5C. *Let G be a minimal preimage of A_k, and fix a surjective homomorphism $\psi : G \to A_k$ with $K := \ker \psi$. Choose $M \leq G$ minimal such that $\psi(M) = A_5 \leq A_k$. Now suppose that $k \geq 10$ and s is an integer such that $k/2 < s < k$, and define $c(k,s) := \binom{s+1}{5}\binom{k}{5}^{-1}$. Then, whenever G acts transitively on a set Ω of size $n < \min\{\binom{k}{s}, \frac{1}{2}\binom{k}{\lfloor k/2 \rfloor}, 2^{\lambda(s+1)}\}$, each element of M fixes at least $c(k,s)n$ points in Ω.*

PROOF. Let $\Sigma := \{\Delta_1, \ldots, \Delta_m\}$ be the set of orbits for K on Ω. Since $K \lhd G$ and G is transitive on Ω, Σ is a system of blocks for G and $|\Delta_i| = n/m$ for each i. Put $H_i := G_{\{\Delta_i\}}$. Then, by Lemma 5.5A (ii), K is a transitive solvable subgroup of H_i. Since $k > 9$ and

$$|A_k : \psi(H_i)| = |G : H_i| = m \leq n < \min\left\{\binom{k}{s}, \frac{1}{2}\binom{k}{\lfloor k/2 \rfloor}\right\}$$

Corollary 5.2A shows that there exists $t \geq s+1$ such that $\psi(H_i)$ has a unique orbit $J_i \subseteq \{1, 2, \ldots, k\}$ of length t and $Alt(J_i) \leq \psi(H_i)$. Choose $M_i \leq H_i$ minimal with respect to the condition that $\psi(M_i) = Alt(J_i)$; so M_i is a minimal preimage of A_t. Since $|\Delta_i| \leq n < 2^{\lambda(s+1)} \leq 2^{\lambda(t)}$, Lemma 5.5B applied to H_i in its action on Δ_i shows that $M_i \leq G_{(\Delta_i)}$.

Now consider the set $I := \{i \mid 1 \leq i \leq m \text{ and } \{1,2,3,4,5\} \subseteq J_i\}$. The definition of M as a minimal preimage of A_5 shows that $M \leq M_i K \leq G_{(\Delta_i)}K$ for all $i \in I$, and because $G_{(\Delta_i)}K/G_{(\Delta_i)}$ is nilpotent by Lemma 5.5A (ii), this shows that $M \leq G_{(\Delta_i)}$ by Lemma 5.5A (iv). Hence we conclude that $\Delta_i \subseteq \mathrm{fix}(M)$ for each $i \in I$, and so each element in M fixes at least $\sum_{i \in I} |\Delta_i| = (n/m)|I|$ points in Ω.

To complete the proof it remains to show that $|I| \geq c(k,s)m$. However, transitivity of G on Σ and of $\psi(G) = A_k$ on the set of t-subsets of $\{1, 2, \ldots, k\}$ shows that each t-subset J of $\{1, 2, \ldots, k\}$ occurs the same number of times, say d times, as a J_i. Hence $m = |\Sigma| = d\binom{k}{t}$ while $|I| = d\binom{k-5}{t-5}$. Thus $|I|/m = \binom{k-5}{t-5}\binom{k}{t}^{-1} = \binom{t}{5}\binom{k}{5}^{-1} = c(k, t-1) \geq c(k,s)$ as required. □

To obtain the bounds we are after, we need some elementary estimates of some binomial coefficients.

Lemma 5.5D. *Let k and s be positive integers with $k \geq 2$ and $s < k$. Suppose that μ is chosen so that $s/(k+1) \leq \mu \leq (s+1)/(k+1)$. Then*

$$\frac{\mu(1-\mu)}{k+1}\rho^{k+1} \leq \binom{k}{s} \leq \rho^{k+1} \quad \textit{where } \rho = \frac{1}{\mu^{\mu}(1-\mu)^{(1-\mu)}}.$$

Proof. Let $t > 0$ and consider the binomial expansion of $(1 + t)^k$. For two successive terms in this expansion we have

$$\binom{k}{i} t^i \le \binom{k}{i+1} t^{i+1} \iff \frac{i+1}{k-i} \le t$$

and so $\binom{k}{s} t^s$ is the largest term whenever $s/(k-s+1) \le t \le (s+1)/(k-s)$. The hypothesis on μ shows that these latter inequalities hold if we put $t = \mu/(1-\mu)$. Now the sum of the terms is $(1+t)^k = (1-\mu)^{-k}$, and there are $k+1$ terms altogether, so we conclude that

$$\frac{(1-\mu)^{-k}}{k+1} \le \binom{k}{s} \mu^s (1-\mu)^{-s} \le (1-\mu)^{-k}.$$

Since $\mu(1-\mu)\rho^{k+1} \le \mu^{-s}(1-\mu)^{-(k-s)} \le \rho^{k+1}$, the stated inequalities follow. □

Theorem 5.5A. *Let G be a permutation group of degree n which contains a section isomorphic to A_k for some $k \ge 10$. Suppose that G has minimal degree at least ωn where $\omega \le 0.4$. Then $n \ge \binom{k}{s}$ for any $s < k$ such that*

$$c(k,s) := \frac{(s+1)s(s-1)(s-2)(s-3)}{k(k-1)(k-2)(k-3)(k-4)} > 1 - \omega.$$

In particular, if we define $s := \lfloor \mu(k+1) \rfloor$ where $\mu := \sqrt[5]{1-\omega}$, then $n > \binom{k}{s}$ for this value of s.

Proof. Let Ω be the set on which G is acting. The hypothesis on G shows that G contains a minimal preimage H of A_k, and Lemma 5.5A (iii) shows that the image of the action of H on each of its nontrivial orbits is also a minimal preimage of A_k. Since G has minimal degree at least $\omega\,|\Omega|$ on Ω, the same must be true for H, so we conclude that the image of H on some nontrivial orbit Γ has minimal degree at least $\omega\,|\Gamma|$. Thus, since $n \ge |\Gamma|$, it is enough to prove the theorem in the special case where G is a minimal preimage of A_k and G is a transitive permutation group.

Next note that $c(k,s) < \{(s+1)/k\}^5$, and so the condition on $c(k,s)$ implies that $s+1 > (\sqrt[5]{1-\omega})k = \mu k$. The hypothesis that $\omega \le 0.4$ shows that $\mu \ge \sqrt[5]{0.6} = 0.9028\ldots$ and so $\min\{\binom{k}{s}, \frac{1}{2}\binom{k}{\lfloor k/2 \rfloor}, 2^{\lambda(s+1)}\} = \binom{k}{s}$ by Exercises 5.5.1 and 5.5.2. We can now apply Lemma 5.5C and the hypothesis on $c(k,s)$ to conclude that n cannot be less than $\binom{k}{s}$. This proves the main assertion.

Finally, if $s := \lfloor \mu(k+1) \rfloor$, then $s+1-i > \mu(k+1) - i > \mu(k-i)$ for $0 \le i \le 4$, because $\mu > 0.8$; hence $c(k,s) > \mu^5 = 1 - \omega$. Thus the hypotheses are satisfied for this choice of s. □

Exercises

5.5.1 Show that $\binom{k}{s} \leq \frac{1}{2}\binom{k}{\lfloor k/2 \rfloor}$ whenever $2(k+1)/3 \leq s \leq k$. [*Hint:* Compare $\binom{k}{s}$ with the preceding binomial coefficient.]

5.5.2 Using the fact that $\lambda(s+1) \geq (2s-2)/3$ (see Theorem 5.7A), show that $\binom{k}{s} \leq 2^{\lambda(s+1)}$ whenever $k \geq 10$ and $0.9k \leq s \leq k$. [*Hint:* Use Lemma 5.5D and the fact that ρ is decreasing as μ increases in the range $0.5 < \mu < 1$.]

Theorem 5.5B. *Let G be a proper 2-transitive permutation group of degree $n \geq 216$. If G contains a section isomorphic to A_k, then $k < 6 \log n$.*

Proof. First note that the result is trivial if $k \leq 32$ since $\log n > 5.37$ for all $n \geq 216$, so we can suppose that $k \geq 33$. Since G is 2-transitive and $n \geq 216$, Theorem 5.4A shows that the minimal degree is at least $n/4$. Applying Theorem 5.5A then shows that $n \geq \binom{k}{s}$ where $\mu = \sqrt[5]{3/4} = 0.9440\ldots$ and $s = \lfloor \mu(k+1) \rfloor$. Now Lemma 5.5D shows that $\binom{k}{s} \geq \frac{\mu(1-\mu)}{k+1}\rho^{k+1}$ where $\rho = 1.2405\ldots$. Hence

$$\log n \geq (k+1)\log\rho + \log\frac{\mu(1-\mu)}{k+1} \geq \left\{0.2155 - \frac{\log(k+1)}{k} - \frac{2.726}{k}\right\}k.$$

This shows that $\log n > k/6$ for all $k \geq 160$. The remaining cases are settled by applying Theorem 5.5A to various ranges of k with s chosen so that $c(k,s) > 1 - 1/4$ (see Table 5.3). This completes the proof of the theorem. □

Table 5.3.

Range of k	s	Minimum value of $c(k,s)$	Minimum value of $\frac{1}{k}\log\binom{k}{s}$
$33 \leq k \leq 39$	$k-2$	$0.8484\ldots$	$0.1694\ldots$
$40 \leq k \leq 63$	$k-3$	$0.7628\ldots$	$0.1680\ldots$
$64 \leq k \leq 87$	$k-4$	$0.7802\ldots$	$0.1679\ldots$
$88 \leq k \leq 112$	$k-5$	$0.7880\ldots$	$0.1670\ldots$
$113 \leq k \leq 136$	$k-6$	$0.7941\ldots$	$0.1675\ldots$
$137 \leq k \leq 161$	$k-7$	$0.7966\ldots$	$0.1671\ldots$

Exercise

5.5.3 Verify the information in Table 5.3. [*Hint:* For a fixed value of i, $c(k, k-i)$ is an increasing function of k, and $\log \binom{k}{k-i} - k/6$ is a decreasing function of k provided $k > 7i$.]

5.6 Bases and Orders of 2-transitive Groups

The following general combinatorial result is useful in a variety of contexts.

Lemma 5.6A. *Let n, d and t be positive integers. Let Ω be a set of size n, and suppose that $\mathcal{F}$ is a family of subsets of Ω such that each $\gamma \in \Omega$ lies in exactly t subsets from $\mathcal{F}$. Then*
(i) *for each $\Gamma \subseteq \Omega$ there exists $\Delta \in \mathcal{F}$ such that $|\Gamma \cap \Delta| \leq |\Gamma| |\Delta| / n$;*
(ii) *if each $\Delta \in \mathcal{F}$ has at least d elements, then for each real $c > 1$ there exists a subfamily $\mathcal{F}_c \subseteq \mathcal{F}$ such that $|\mathcal{F}_c| < (n \log c)/d + 1$ and*

$$\left| \bigcup_{\Delta \in \mathcal{F}_c} \Delta \right| > \left(1 - \frac{1}{c}\right) n$$

PROOF. (i) Let $\mathcal{F}(\gamma)$ denote the set of $\Delta \in \mathcal{F}$ with $\gamma \in \Delta$, and note that $|\mathcal{F}(\gamma)| = t$ by hypothesis. Then

$$\sum_{\Delta \in \mathcal{F}} |\Gamma \cap \Delta| = \sum_{\gamma \in \Gamma} |\mathcal{F}(\gamma)| = t |\Gamma| .$$

In particular, substituting Ω for Γ gives

$$\sum_{\Delta \in \mathcal{F}} |\Delta| = tn.$$

Hence, for general Γ, we have

$$t |\Gamma| = \sum_{\Delta \in \mathcal{F}} \frac{|\Gamma \cap \Delta|}{|\Delta|} |\Delta| \geq \frac{|\Gamma \cap \Delta^*|}{|\Delta^*|} \sum_{\Delta \in \mathcal{F}} |\Delta|$$

for some $\Delta^* \in \mathcal{F}$, and (i) follows.

(ii) Define subsets $\Gamma_0, \Gamma_1, \ldots$ of Ω as follows. Put $\Gamma_0 := \emptyset$. For each $i \geq 0$ we use (i) to choose $\Delta_i \in \mathcal{F}$ such that

$$|\Gamma_i \cap \Delta_i| \leq |\Gamma_i| |\Delta_i| / n$$

and put $\Gamma_{i+1} := \Gamma_i \cup \Delta_i$ and $g_i := |\Gamma_i|$. Clearly $g_{i+1} > g_i$ as long as $\Gamma_i \neq \Omega$. We claim that if we stop at the index k where $g_k > (1 - 1/c)n \geq g_{k-1}$ then $k < (n \log c)/d + 1$. Since the latter inequality is trivial for $k = 1$, we can suppose that $k \geq 2$. The choice of Δ_i shows that for each i

$$n - g_{i+1} \leq n - g_i - |\Delta_i| \left(1 - \frac{g_i}{n}\right) \leq (n - g_i)\left(1 - \frac{d}{n}\right).$$

Since $g_0 = 0$ and $k \geq 2$, this shows that

$$\frac{n}{c} \leq n - g_{k-1} \leq n\left(1 - \frac{d}{n}\right)^{k-1} < n\exp\left\{\frac{-d\,(k-1)}{n}\right\}.$$

Therefore $-\log c = \log(1/c) < -d(k-1)/n$ and the result is proved. □

Lemma 5.6B. *Suppose that $G \leq Sym(\Omega)$ has degree $n \geq 2$ and that $k \geq 5$. If G does not have a section isomorphic to A_k, then there exists $\Delta \subseteq \Omega$ with $|\Delta| \leq 2k$ such that every orbit of $G_{(\Delta)}$ has length less than $0.63n$.*

PROOF. Suppose that no such set Δ exists. To simplify notation, put $b := 0.63$. Then we can define a sequence of subgroups $G(i)$ $(i = 0, \ldots, 2k)$ of G such that $G(0) = G$ and, for each $i \geq 1$, the group $G(i)$ is a point stabilizer of $G(i-1)$ with $|G(i-1) : G(i)| \geq bn$ (choose the point to lie in the largest orbit of $G(i-1)$). Then $G(2k) = G_{(\Delta)}$ for some subset Δ of size $2k$, and $\left|G : G_{(\Delta)}\right| \geq (bn)^{2k}$. On the other hand, considering the action of G on the set $\Omega^{\{2k\}}$ of $2k$-subsets, we have

$$\left|G : G_{\{\Delta\}}\right| \leq \left|\Omega^{\{2k\}}\right| = \binom{n}{2k}$$

and so

$$\left|G_{\{\Delta\}} : G_{(\Delta)}\right| \geq \binom{n}{2k}^{-1} (bn)^{2k} = \frac{(2k)!\; n^{2k}\; b^{2k}}{n(n-1)\cdots(n-2k+1)} > (2k)!\; b^{2k}.$$

Now the restriction map gives a homomorphism of

$$G_{\{\Delta\}} \to Sym(\Delta) \cong S_{2k}$$

with kernel $G_{(\Delta)}$ and image $H := G^{\Delta}_{\{\Delta\}} \cong G_{\{\Delta\}}/G_{(\Delta)}$. By the hypothesis on G, the group H cannot contain a subgroup isomorphic to A_k. Since $k > 4$, this implies that the index of H in $Sym(\Delta)$ is at least $\binom{2k}{k}$ by Theorem 5.2B. Therefore

$$|H| = \left|G_{\{\Delta\}} : G_{(\Delta)}\right| \leq \frac{(2k)!}{\binom{2k}{k}}.$$

As we saw in the proof of Lemma 5.1A, $\binom{2k}{k} \geq 2^{2k}/2k$. Using this together with the last two inequalities for $\left|G_{\{\Delta\}} : G_{(\Delta)}\right|$ we conclude that $(2b)^{2k} < 2k$. Since $(2k)^{1/2k} \leq 10^{1/10} < 1.26 = 2b$ for all $k \geq 5$, this gives a contradiction. Thus there exists a set Δ for which $G_{\{\Delta\}}$ has all its orbits of size $< bn$, and the lemma is proved. □

Lemma 5.6C. *Let $G \leq Sym(\Omega)$ be 2-transitive of degree $n \geq 6$, and let b be a constant with $0 < b < 1$.*

(i) *If there exists a set $\Sigma \subseteq \Omega$ such that $G_{(\Sigma)}$ has no orbit of length $> bn$, then G has a base of size at most*

$$\left\{ \frac{2}{1-b} \log n + 1 \right\} |\Sigma| .$$

(ii) *If $k \geq 5$ and G does not have a section isomorphic to A_k, then G has a base of size at most $12k \log n$.*

PROOF. (i) Let

$$\Delta := \left\{ (\alpha, \beta) \in \Omega^{(2)} \mid \alpha, \beta \text{ lie in distinct } G_{(\Sigma)}\text{-orbits} \right\}.$$

Then the hypothesis on $G_{(\Sigma)}$ shows that

$$|\Delta| \geq \sum_{\alpha \in \Omega} (1-b)n = (1-b)n^2.$$

Consider the family $\mathcal{F}$ of sets Δ^x indexed by $x \in G$. Because G is 2-transitive, each pair $(\alpha, \beta) \in \Omega^{(2)}$ lies in the same number of sets in $\mathcal{F}$ and so we can apply Lemma 5.6A (ii) with $c = n^2$. We conclude that there is a subset $T \subseteq G$ with

$$|T| < \frac{n(n-1) \log c}{(1-b)n^2} + 1 < \frac{2}{1-b} \log n + 1$$

such that $\bigcup_{x \in T} \Delta^x = \Omega^{(2)}$. Since

$$(\alpha, \beta) \in \Delta^x \iff \alpha, \beta \text{ lie in distinct } G_{(\Sigma^x)}\text{-orbits}$$

we conclude that $\Gamma := \bigcup_{x \in T} \Sigma^x$ is a base for G with

$$|\Gamma| < \left\{ \frac{2}{1-b} \log n + 1 \right\} |\Sigma| .$$

This proves (i).

(ii) Lemma 5.6B shows that the hypotheses of part (i) hold with $|\Sigma| = 2k$ and $b = 0.63$. Hence we can find a base of size at most

$$2k \left\{ \frac{2}{0.37} \log n + 1 \right\} < 12k \log n$$

since $\log n \geq \log 6 > 1.79$. □

Theorem 5.6A. *If G is a proper 2-transitive subgroup of degree n, then G has a base of size at most $72(\log n)^2$. Hence the order of G is at most $\exp\{72\ (\log n)^3\}$.*

PROOF. The result is trivially true for $n < 216$, so we can suppose $n \geq 216$. Then from Theorem 5.5B, G does not have A_k as a section if

$k \geq 6 \log n$. Hence part (ii) of the preceeding lemma gives the desired conclusion. □

Since $(\log n)^2$ grows more slowly than $\sqrt{n}$ we can combine Theorems 5.6A and 5.3A to get the following bound valid for any proper primitive group.

Theorem 5.6B. *There exists a constant $c' > 0$ such that every proper primitive group of degree n has order at most* $\exp\{c'\sqrt{n}(\log n)^2\}$.

It is possible, but not very enlightening, to make an estimate of the value of c'. It is certainly much too large to be useful for moderate degrees, say less than a million. There is an alternative bound known for the order of a proper primitive group of degree n, namely 4^n. This is poorer as an asymptotic bound but has the advantage of being valid for all degrees. The proof of this result which is due to Wielandt (1969) and Praeger and Saxl (1980) is quite different from the proofs given above; it is less combinatorial and uses more of the group structure.

However neither of these results really describes the true picture, and Liebeck (1984b) has used the classification of finite simple groups to prove the following.

Theorem 5.6C (Assuming the classification of finite simple groups). *Let G be a primitive group of degree n. Then there is a constant $b > 0$ (which can be taken to be $9/(\log 2)$) such that at least one of the following holds:*

(i) *there are positive integers d, k and m such that G has a socle which is permutation isomorphic to A_m^d where the action of A_m is equivalent to its action on k-element subsets of $\{1, \ldots, m\}$ and $n = \binom{m}{k}^d$; or*

(ii) *G has a base of size less than $b \log n$ and so has minimal degree greater than $n/(b \log n)$ and order less than* $\exp(b(\log n)^2)$.

Exercises

5.6.1 Show that $AGL_d(2)$ has a base of size approximately $(\log n)/(\log 2)$ so the bounds in part (ii) of the theorem above are within a constant factor of being best-possible.

5.6.2 Let G be a finite group acting transitively on a finite set Ω of size $n \geq 3$, and fix $\alpha \in \Omega$. Show that for some integer $t < (\log n + \log\log n)/\log 2 + 1$ there exist elements $x_1, \ldots, x_t \in G$ such that each point in Ω has the form α^z where $z = x_1^{\epsilon_1} \ldots x_t^{\epsilon_t}$ with $\epsilon_i \in \{0, 1\}$ for each i. In particular (taking the action as right multiplication on G), there is a set of t generators $x_1, \ldots, x_t$ of G such that each element $z \in G$ has the form described. [*Hint:* Apply Lemma 5.6A.]

5.7 The Alternating Group as a Section of a Linear Group

The present section is devoted to obtaining a lower bound on the dimension d of the general linear groups $GL_d(F)$ which contain finite preimages of A_k. This is necessary to complete the proofs of Sect. 5.5. We begin with some general results. Recall that a group is locally finite if every finitely generated subgroup is finite. In particular, finite groups and infinite abelian p-groups are locally finite.

Lemma 5.7A. *If G is a finite p-group which acts as a group of automorphisms on a locally finite p-group $H \neq 1$, then* $\mathrm{fix}_H(G) \neq \{1\}$.

PROOF. Take any $u \neq 1$ in H, and define $K := \langle u^x \mid x \in G \rangle$. Then K is a finite nontrivial p-subgroup of H by the hypotheses and K is G-invariant. Since the nontrivial orbits of G all have lengths divisible by p, the set $\mathrm{fix}_K(G)$ of fixed points on K satisfies

$$|\mathrm{fix}_K(G)| \equiv |K| \equiv 0 \pmod{p}.$$

Since $1 \in \mathrm{fix}_K(G)$, we conclude that $|\mathrm{fix}_H(G)| \geq |\mathrm{fix}_K(G)| \geq p$. □

Suppose that G acts as a group of automorphisms of H and that H has a finite chain of subgroups

$$H = H_0 \geq H_1 \geq \ldots \geq H_r = 1. \tag{5.6}$$

Then we say that G *stabilizes* the chain (5.6) if for each i, $1 \leq i \leq r$, we have: (i) H_i is G-invariant, and (ii) for all $u \in H_{i-1}$, $H_i u = H_i u^x$ for all $x \in G$.

Lemma 5.7B.

(i) *Suppose that θ is a p-element in* $\mathrm{Aut}(H)$ *for some prime p, and $\langle\theta\rangle$ stabilizes the chain (5.6). If H contains no nontrivial p-element, then $\theta = 1$.*

(ii) *Let G be a minimal preimage of A_k $(k \geq 5)$, and suppose that H is a group in which every nontrivial element either has infinite order or has q-power order for some fixed prime q. If G acts on H as a group of automorphisms and G stabilizes the chain (5.6), then G acts trivially on H.*

PROOF. (i) The result is clearly true if $r \leq 1$, so proceed by induction on r, and assume $r > 1$. Since H_1 is invariant under θ, the group $\langle\theta\rangle$ acts as a group of automorphisms on H_1 and hence θ acts trivially on H_1 by induction. Now for each $u \in H$, there exists $z \in H_1$ such that $u^\theta = zu$, and hence $u^{\theta^i} = z^i u$ for $i = 1, 2, \ldots$. If θ has order m, then this shows that $u = z^m u$, and so $z^m = 1$. Since m is a power of p, z must be a p-element,

and so $z = 1$ by the hypothesis on H. Hence $u^\theta = u$ for all $u \in H$, and so $\theta = 1$.

(ii) Choose any prime $p \leq k$ with $p \neq q$. Let $x \in G$ be a p-element which maps onto a nontrivial p-element of A_k. Now (i) shows that the kernel of the action of G on H contains x, hence the kernel is G by Lemma 5.5A. □

We shall require some elementary results from linear algebra. Let F be an algebraically closed field and let V be a d-dimensional vector space over F. Let $\mathrm{End}(V)$ denote the ring of all F-linear transformations (or endomorphisms) of V into itself; recall that this is also a vector space of dimension d^2 over F. The invertible linear transformations in $\mathrm{End}(V)$ form the group $GL(V)$. A linear transformation $t \in \mathrm{End}(V)$ is called *diagonalizable* if t has a diagonal matrix relative to some basis for V. The following results are well known (see, for example, Hoffman and Kunze (1971) Sect. 6.4 and 6.5).

Lemma 5.7C.

(i) *$t \in \mathrm{End}(V)$ is diagonalizable $\iff$ the minimal polynomial $m(X)$ for t has distinct roots. In particular, if $t^n = 1$, then $m(X) \mid X^n - 1$. If char $F = 0$ or char $F = q > 0$ but $q \nmid n$, then* $\mathrm{GCD}(X^n - 1, nX^{n-1}) = 1$, *and so $X^n - 1$ has distinct roots. Thus in this case $t^n = 1$ implies that t is diagonalizable.*

(ii) *If T is a set of diagonalizable linear transformations which commute with one another, then there is a basis for V over which all $t \in T$ have diagonal matrices simultaneously.*

Exercises

5.7.1 Let G be a subgroup of $GL(V)$ over the field F.
   (i) If $t \in \mathrm{End}(V)$ commutes with every element of G, then $\ker t$ and $\mathrm{Im}\, t$ are G-invariant subspaces of V.
   (ii) If the only G-invariant subspaces are V and 0, and F is algebraically closed, then $Z(G)$ consists of scalar matrices of the form $\zeta 1$.
   (iii) If char $F = p \neq 0$, then 1 is the only p-element in $GL(V)$ which is a scalar.

   [*Hint:* In the second part, if $z \in Z(G)$, consider $z - \zeta 1$ where ζ is an eigenvalue ζ for z. For the third part use the fact that $(X-1)^{p^r} = X^{p^r} - 1$ over any field of characteristic p.]

5.7.2 Let G be any group, and for each $x \in G$ define

$$C_G^*(x) := \{y \in G \mid [x,y] \in Z(G)\}.$$

Prove that $C_G^*(x)$ is a subgroup of G and that $y \mapsto [x,y]$ is a homomorphism from $C_G^*(x)$ into $Z(G)$ with kernel $C_G(x)$. In particular, $C_G^*(x)/C_G(x)$ is abelian.

5.7.3 Show that there is no field for which $SL_2(F)$ contains a finite preimage G of A_6. [*Hint:* If char $F \neq 3$ then every finite 3-subgroup of $SL_2(F)$ is cyclic, while if char $F = 3$ then the elements of order 2 lie in the centre, and so G would have an element of order 12.]

5.7.4 Show that there is no field for which $SL_3(F)$ contains a finite preimage G of A_7.

We define $\lambda(k)$ to be the smallest positive integer d for which there exists a field F such that $GL_d(F)$ contains a finite preimage G of A_k. Simple arguments show that $\lambda(k) \leq k-1$ for all $k \geq 2$, and that $\lambda(2) = \lambda(3) = 1$ and $\lambda(4) = \lambda(5) = 2$. Obviously there is no restriction in assuming that F is algebraically closed. Our object is to obtain a general lower bound on $\lambda(k)$.

Theorem 5.7A. *For all $k \geq 2, \lambda(k) \geq (2k-4)/3$.*

A major part of the proof of this theorem is the proof of the following lemma.

Lemma 5.7D. *Let $k \geq 5$, and let $d = \lambda(k)$. Then there exists an algebraically closed field F and a finite subgroup G of $SL_d(F)$ such that:*
(i) *G is irreducible as a linear group;*
(ii) *$Z(G)$ is a group of scalars $\zeta 1$ (with $\zeta \in F$) and its order divides d;*
(iii) *if char $F = p > 0$, then $p \nmid |Z(G)|$;*
(iv) *$G/Z(G) \cong A_k$.*

PROOF. The definition of d shows that there exists an algebraically closed field F such that $GL_d(F)$ contains a finite preimage G of A_k. We choose F and G so that G has smallest possible order; let K be the kernel of this preimage. Note that G must be a minimal preimage of A_k and hence $G' = G$ because $k \geq 5$. Since $\det(x^{-1}y^{-1}xy) = 1$ for all $x, y \in G$, this shows that $G \leq SL_d(F)$.

Let $V = F^d$ denote the underlying vector space. Since $GL(V) \cong GL_d(F)$, we can identify G with its image in $GL(V)$. We shall now show that G satisfies the conditions (i)–(iv).

(i) Suppose that W is a G-invariant subspace. Then G stabilizes the subgroup chain $V \supseteq W \supseteq 0$ of $(V, +)$. Since G does not act trivially on V, Lemma 5.7B (ii) shows that G does not act trivially on both W and V/W, and so, by Lemma 5.5A (iii) and the choice of G, must act faithfully on one of these. Now the minimality of d shows that either W or V/W has dimension d, and so $W = 0$ or V. This proves (i).

(ii) Since G acts irreducibly on V, Exercise 5.7.1 shows that $Z(G)$ is a group of scalars. Thus $Z(G) \leq \{\zeta 1 \mid \zeta^d = 1\}$ because $G \leq SL_d(F)$. In particular, $|Z(G)|$ divides d.

(iii) Suppose that char $F = p > 0$, and let P be a Sylow p-subgroup of K. Since P acts on the locally finite p-group $(V, +)$ as a group of automor-

phisms, Lemma 5.7A shows that $W := \mathrm{fix}_V(P) \neq 0$. Since P is the unique Sylow p-subgroup of K by Lemma 5.5A (ii), therefore $P \lhd G$. Hence W is a G-invariant subspace, and so $W = V$ by the irreducibility of G. Hence $\mathrm{fix}_V(P) = V$, and so $P = 1$. This shows that $p \nmid |K|$. Since $Z(G) \leq K$, (iii) follows.

(iv) We have to show that $K = Z(G)$. Suppose that this is false. Since K is nilpotent by Lemma 5.5A (ii), there exists a subgroup M of K such that $M/Z(G)$ is a minimal normal subgroup of $G/Z(G)$ contained in $Z(K/Z(G))$. Then $M/Z(G)$ is an elementary abelian group of order q^r, say, for some prime q. We claim that $r \leq d$.

First, if $M \leq Z(K)$, then M is abelian and, as we saw in the proof of (iii) above, the order of K is relatively prime to the characteristic of F if the latter is nonzero. Since F is algebraically closed and M is abelian, we can find a basis of V over which all elements of M correspond to diagonal matrices by Lemma 5.7C (ii). Each finite subgroup of the multiplicative group of any field is cyclic (see, for example Lang (1993) IV §1), so we have an embedding of M into a direct product of (at most) d cyclic groups. Hence M itself is generated by at most d elements, and so the same is true for the homomorphic image $M/Z(G)$. Hence $r \leq d$ in this case.

Second, if M is not contained in $Z(K)$, then $M \cap Z(K) = Z(G)$ by the minimality of M. Choose elements $x_1, \dots, x_m$ from M to form an F-basis of the subspace of $\mathrm{End}(V)$ spanned by M (so $m \leq d^2$). The elements of this basis lie in different cosets of $Z(G)$ because $Z(G)$ consists of scalars; we shall show that in fact they form a set of coset representatives for $Z(G)$ in M. Indeed, if this were not true then we could choose $y \in M$ such that no x_i lies in the coset $Z(G)y$. Then $y = \sum \lambda_i x_i$ for some unique $\lambda_i \in F$, and so $1 = \sum \lambda_i x_i y^{-1}$. Since $x_i y^{-1}$ does not lie in $Z(G)$, it is not contained in $Z(K)$ and so we can choose $z_i \in K$ which does not commute with $x_i y^{-1}$. Since $M/Z(G) \leq Z(K/Z(G))$ and $Z(G)$ consists of scalars, this shows that there exist $\zeta_{ij} \in F$ such that

$$[x_i y^{-1}, z_j] = \zeta_{ij} 1 \quad \text{and} \quad \zeta_{ii} \neq 1 \quad \text{for } i, j = 1, \dots, m.$$

Thus, for each j, we have

$$1 = z_j^{-1} 1 z_j = \sum \lambda_i z_j^{-1} x_i y^{-1} z_j = \sum \lambda_i \zeta_{ij} x_i y^{-1}.$$

The linear independence of the x_i now shows that $\lambda_j \zeta_{jj} = \lambda_j$ for each j, and so $\lambda_j = 0$ because $\zeta_{jj} \neq 1$. This implies $y = 0$, and we have a contradiction. Hence $x_1, \dots, x_m$ is a set of coset representatives for $Z(G)$ in M and so

$$d^2 \geq m = |M : Z(G)| = q^r \geq 2^r$$

which shows that $r \leq d$ in this case as well.

Thus we have shown that $M/Z(G)$ is a vector space of dimension $\leq d$ over the field with q elements. Since the kernel of G acting on this space (by conjugation) contains M, Lemma 5.5A (iii) and the minimality of $|G|$ in

the choice of G shows that G must act trivially on this space. Now, Lemma 5.7B (ii) shows that G acts trivially on the Sylow q-subgroup of M, and so $M \leq Z(G)$ contrary to hypothesis. This shows that $Z(G)$ must be all of K as claimed. □

PROOF OF THEOREM 5.7A. We proceed by induction on k. The cases where $k \leq 7$ are dealt with in Exercises 5.7.3 and 5.7.4, so suppose $k \geq 8$. Let $d := \lambda(k)$, and let $G \leq SL_d(F)$ be a group satisfying the conditions (i)–(iv) of Lemma 5.7D for a suitable field F. Since $k \geq 8$, we have $d \geq 4$ by Exercise 5.7.4. Let ϕ denote a homomorphism of G onto A_k, and choose x in a Sylow 3-subgroup of G such that $\phi(x) = (123) \in A_k$. With the notation of Exercise 5.7.2

$$C_G^*(x)/Z(G) \cong C_{A_k}((123)) \cong \langle(123)\rangle \times A_{k-3}$$

and $C_G^*(x)/C_G(x)$ is abelian, so $C := C_G(x)$ has a section isomorphic to the simple group A_{k-3} (recall that $k-3 \geq 5$ because $k \geq 8$). Let H be a minimal preimage of A_{k-3} in C.

Put $V := F^d$. If $V = V_0 \geq V_1 \geq V_2 \ldots \geq V_r = 0$ is any chain of C-invariant subspaces, then H must act nontrivially on at least one of the factor spaces V_{i-1}/V_i, since otherwise H would not act faithfully on V by Lemma 5.7B (ii). Thus, if we can prove that there exists a chain of C-invariant subspaces in which successive quotient spaces all have dimension $\leq d-2$, then induction shows that $d - 2 \geq \{2(k-3)-4\}/3$ and hence $d \geq (2k-4)/3$ as required. To complete the proof we consider two cases.

First, suppose that char $F \neq 3$. In this case x is diagonalizable. Since each eigenspace of x is C-invariant (Exercise 5.7.1), it is enough to show that x does not have an eigenspace of dimension $d-1$. Suppose the contrary; then x corresponds to a diagonal matrix of the form $\mathrm{diag}(\alpha, \beta, \ldots, \beta)$. Choose $y \in G$ such that $\phi(y) = (12)(45) \in A_k$. Then the conjugate $y^{-1}xy$ of x has the form $x^2\zeta$ because $\phi(y^{-1}xy) = \phi(x)^2$ and the elements of $Z(G)$ are scalars. Thus the diagonal matrix for x is similar to $\mathrm{diag}(\alpha^2\zeta, \beta^2\zeta, \ldots, \beta^2\zeta)$ and so the diagonal entries of the two matrices must match after possible reordering. Since $d > 2$, this can only happen if $\alpha = \alpha^2\zeta$ and $\beta = \beta^2\zeta$. Hence $\alpha = \zeta^{-1} = \beta$, which is impossible because x does not lie in $Z(G)$. Hence every eigenspace for x has dimension $\leq d-2$ and the proof is completed in this case.

Second, suppose that char $F = 3$. In this case $3 \nmid |Z(G)|$ by Lemma 5.7D, and so x is an element of order 3 in G. Thus the minimal polynomial for x divides $X^3 - 1 = (X-1)^3$ (compare with Exercise 5.7.1). Hence all the eigenvalues of x equal 1, and the blocks in the Jordan canonical form for x have one of the three forms:

$$[1], \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

A simple calculation shows that the dimension of $W := \ker(x-1)$ is equal to the number of Jordan blocks, and so is at least 2 (since $d \geq 4$) and at most $d-1$. Since W is C-invariant the only case we have to consider is when $\dim W = d-1$, and this occurs only when x has one block of size 2 and all other blocks of size 1. In this case we see that $U := \mathrm{Im}(x-1)$ is a C-invariant subspace of dimension 1 contained in W, and so the chain $V > W > U > 0$ fulfills our requirements.

Thus we have proved the induction step in all cases, and hence completed the proof of the theorem. □

5.8 Small Subgroups of S_n

The following theorem is an application of some of the results obtained in this chapter to show that many interesting classes of groups always appear as small subgroups of S_n.

Theorem 5.8A. *Let $\mathcal{C}$ be a nonempty class of finite groups with the property that whenever $G \in \mathcal{C}$ then every subgroup and homomorphic image of G lies in $\mathcal{C}$. (Briefly: $\mathcal{C}$ is closed under taking subgroups and homomorphic images.) Suppose that $\mathcal{C}$ does not contain every finite group. Then there exists $c > 1$ such that for all $n \geq 1$:*

$$\text{(5.7)} \qquad \textit{if } G \leq S_n \textit{ and } G \in \mathcal{C}, \textit{ then } |G| \leq c^{n-1}.$$

PROOF. Since $\mathcal{C}$ does not contain every finite group and is closed under taking isomorphisms and subgroups, there exists m such that $A_m \notin \mathcal{C}$. Choose $c_0 > 1$ such that (5.7) holds with $c = c_0$ for all $n \leq m$. Now choose $n_0 \geq m$ such that (5.7) holds with $c = c_0$ whenever G is primitive and $n \geq n_0$. This is possible because the choice of m and the hypothesis on $\mathcal{C}$ ensures that G must be a proper primitive subgroup of S_n when $n > n_0$, and so Theorem 5.6B applies. Finally choose $c \geq c_0$ so that (5.7) holds for all $n \leq n_0$. We claim (5.7) now holds for all values of n.

Indeed, (5.7) holds when G is primitive by the choice of c, and also for small values of n, so we can proceed by induction on n assuming that G is either imprimitive or intransitive. If $G \leq S_n$ is imprimitive, then there exists $d \mid n$ with $1 < d < n$ such that G can be embedded in a wreath product of the form $H \text{ wr } K$ where $H \leq S_{n/d}$ is isomorphic to a subgroup of G and $K \leq S_d$ is isomorphic to a factor group of G (Exercise 2.6.2). Thus the hypothesis on $\mathcal{C}$ together with the induction hypothesis implies that

$$|G| \leq |H|^d |K| \leq c^{(n/d-1)d} c^{d-1} = c^{n-1}$$

as required. On the other hand, if $G \leq S_n$ is intransitive, a similar argument shows that G can be embedded in a direct product $H \times K$ where $H \leq S_d$ and $K \leq S_{n-d}$ for some d with $1 \leq d \leq n-1$, and H and K are

homomorphic images of G. Then the hypothesis on $\mathcal{C}$ and the induction hypothesis show that $|G| \leq |H|\,|K| \leq c^{d-1}c^{n-d-1} < c^{n-1}$, so the induction step is proved in this case too. This proves the theorem. □

Exercises

5.8.1 Suppose that in addition to the hypothesis of the theorem, we assume that $\mathcal{C}$ is closed under taking direct products, and that $\mathcal{C}$ contains a nontrivial group. Show that in this case there exists $c' > 1$ such that, for infinitely many values of n, there exists $G \leq S_n$ with $G \in \mathcal{C}$ such that $|G| \geq (c')^{n-1}$. Hence there exists some $c > 1$ such that (5.7) holds for all $n \geq 1$ and such that, for each c' with $1 < c' < c$, there exists infinitely many n for which (5.7) fails to hold if c is replaced by c'.

5.8.2 Show that every abelian subgroup of S_n has order at most c^n where $c = 3^{1/3} = 1.44225\ldots$ and that this bound is reached whenever n is a multiple of 3.

5.8.3 Find a similar bound for the nilpotent subgroups of S_n.

5.8.4 Suppose that in addition to the hypothesis of the theorem we assume that $\mathcal{C}$ is closed under forming extensions (that is, if $N \lhd G$ with $N \in \mathcal{C}$ and $G/N \in \mathcal{C}$, then $G \in \mathcal{C}$). Prove that there exist $c \geq 1$ such that (5.7) holds for all $n \geq 1$, with the bound exact for infinitely many n.

5.8.5 Prove that every subgroup $G \leq S_n$ of odd order has its order bounded by $3^{(n-1)/2}$ and that this bound is exact whenever n is a power of 3. [*Hint:* If G is primitive, the point stabilizer G_α acts faithfully on a set of size $(n - 1)/2$ (see Theorem 4.4A (ii)).]

In the special case where $\mathcal{C}$ is the class of solvable groups, we can make the conclusion of Theorem 5.8A more precise.

Theorem 5.8B. *Let* $c := 24^{1/3} = 2.8845\ldots$. *Then, for every permutation group G of degree n, the product of the orders of the abelian factors in a composition series for G is at most c^{n-1}. In particular, the solvable subgroups of S_n have order at most c^{n-1}.*

PROOF. We shall first prove the result in the special case where G is solvable. It is easy to check that the result is true for $n \leq 4$ (the bound is exact for $n = 1$ and $n = 4$), so we shall proceed by induction on n, and assume $n > 4$. We consider three cases.

(i) If G is intransitive with an orbit of length d, say, with $1 \leq d < n$, then G is isomorphic to a subgroup of $S_d \times S_{n-d}$. Thus, by induction, $|G| \leq c^{d-1}c^{n-d-1} < c^{n-1}$.

(ii) If G is imprimitive, then there exists $d \mid n$ with $1 < d < n$ and $m := n/d$ such that G is isomorphic to a subgroup of the wreath product $S_d \text{ wr } S_m$ with the natural action of S_m. Then induction shows that $|G| \leq (c^{d-1})^m c^{m-1} = c^{n-1}$.

(iii) If G is primitive, then $n = p^k$, say is a power of some prime p, G has an abelian socle of order p^k, and G_α is isomorphic to some subgroup of $GL_k(p)$ (see Theorem 4.6A). Hence

$$|G| = p^k |G_\alpha| \leq p^k(p^k - 1)(p^k - p) \cdots (p^k - p^{k-1}) < n^{k+1}.$$

Now

$$(k+1)\log n = \log pn \log n / \log p \leq \log 2n \log n / \log 2.$$

A simple calculus argument shows that the last expression is less than $(n-1)\log c$ whenever $n \geq 16$; so $n^{k+1} < c^{n-1}$ for $n \geq 16$ and the required bound is proved for these values of n. Direct verification shows that the latter inequality also holds for each prime power $n = p^k$ with $5 \leq n \leq 13$ except for $n = 8$. Finally, for $n = 8$, $|G| \leq 8\,|GL_3(2)| = 1344 < c^7$, and so the bound holds for all degrees. This completes the proof of the theorem in the special case where G is solvable.

Now consider the case where $G \leq S_n$ is a general permutation group of degree n. It is enough to consider the case where G is chosen so that the product of the orders of its abelian composition factors is as large as possible for a group of this degree while the order of G is as small as possible. We claim that in this case G is solvable. Indeed, if G is not solvable, then there exist normal subgroups H and K of G such that: $K \leq H, G/H$ is solvable, and H/K is a nonabelian chief factor of G (and hence a direct product of nonabelian simple groups). Let P/K be a nontrivial Sylow p-subgroup of H/K. Then the Frattini argument (Exercise 1.4.14) shows that $G = NH$ where $N/K := N_{G/K}(P/K)$. Now $K \leq N$ and N/K has a quotient $N/(N \cap H) \cong G/H$. Hence the product of the orders of the abelian composition factors of N is as great as the corresponding product for G while $|N| < |G|$. Since this contradicts the choice of G, we conclude that G must be solvable. Thus the bounds for the special case apply in the general case, and the theorem is proved. □

Exercises

5.8.6 Show that the bound in the theorem above is attained for groups of degree 4^k.

5.8.7 Show that every solvable subgroup of S_n has its derived length $\ell(G)$ bounded by $\lfloor b \log n \rfloor$ where $b = 5/(2\log 3) = 2.27559\ldots$, and that this bound is best possible whenever n is a power of 9.

5.9 Notes

- Theorem 5.1A and Exercises 5.1.4–6: It is shown in Landau (1909) §61 that $\log h_n$ is asymptotic to $\sqrt{n \log n}$ as $n \to \infty$. See also Nicolas (1967), Miller (1987) and Massias et al. (1989).
- Theorem 5.1B: See Babai and Seress (1987).

- Theorems 5.2A and 5.2B: See Liebeck (1983b) and Jordan (1870) 68–75.
- Exercise 5.2.8: See also Sect. 8.5.
- Lemmas 5.3A and 5.3B: See Babai (1980) and (1981).
- Theorem 5.3A: See Babai (1981).
- Theorem 5.4A and Lemma 5.4B: See Bochert (1897).
- Exercise 5.4.3: Known to Jordan. See also Babai and Seress (1987).
- Sect. 5.5: This section is based on Wielandt (1934). Theorem 5.5B gives a logarithmic bound on the degree of transitivity of a finite permutation group; this was the original aim of Wielandt (1934). All significantly better bounds on degree of transitivity use (directly or indirectly) the classification of finite simple groups; see Sect. 7.3.
- Lemma 5.6A and Exercise 5.6.2: See Babai and Erdös (1982).
- Lemma 5.6B, Lemma 5.6C and Theorem 5.6A: See Pyber (1993a) and (1995) which are based on Babai (1982). Babai gives a weaker version of Theorem 5.6B. For related results see Pyber (1993b).

  Wielandt (1969) proves that the order of a simply primitive group of degree n is at most 24^n. Praeger and Saxl (1980) improved this bound to 4^n, and showed that it holds for all proper primitive groups of degree n. (The proof, however, is very computational, and not all the details are spelled out.) The Wielandt–Praeger–Saxl bound is useful because it is nontrivial even for relatively small values of n, in contrast to the asymptotically better bounds of Theorems 5.3A and 5.6A. For related bounds for transitive groups see Liebeck (1982) and (1984a).
- Sect. 5.7: The whole object of this section is to prove the inequality of Theorem 5.7A and so complete the proof of Theorem 5.5B. The bound which we obtain is not tight. Indeed, Lemma 5.7D shows that $\lambda(k)$ is the minimal degree of a projective linear representation of A_k, and using information about these representations [see Hoffman and Humphreys (1992)] it can be shown that $\lambda(k) \geq k - 2$.
- Theorem 5.8A: Using the Wielandt-Praeger-Saxl bound discussed above, Babai et al. (1982) proves that if $k \geq 6$ and $G \leq S_n$ has no section isomorphic to A_k, then $|G| \leq k^n$.
- Exercise 5.8.5: See Alspach (1968) for a purely combinatorial proof.
- Theorem 5.8B: See Dixon (1967) for the solvable case. See also Palfy (1982).

6

The Mathieu Groups and Steiner Systems

6.1 The Mathieu Groups

The five Mathieu groups, $M_{11}, M_{12}, M_{22}, M_{23}$ and M_{24}, are a truly remarkable set of finite groups. These groups were first described in papers of Emile Mathieu (1861, 1873), and are the only finite 4- and 5-transitive groups which are not alternating or symmetric. Moreover, all five of the Mathieu groups are simple, and constitute the earliest known examples of sporadic simple groups (simple groups not belonging to an infinite family). The five Mathieu groups are all subgroups of M_{24}. In recent decades, M_{24} has been used to construct exceptionally tight packings of spheres in $\mathbb{R}^{24}$ which in turn have led to a number of further sporadic finite simple groups [see Thompson (1983)].

The group M_{12} is *sharply* 5-transitive of degree 12, which means that each 5-point stabilizer is the identity. The group M_{11} as a point stabilizer of M_{12}; so M_{11} in turn is sharply 4-transitive on 11 points. Indeed the stabilizer of a point in M_{11} is a group, sometimes called M_{10}, which is isomorphic to $A_6 \cdot 2$. The group M_{11} also has an exceptional 3-transitive permutation action on 12 points with the point stabilizers isomorphic to $PSL_2(11)$. Thus $PSL_2(11)$ has both its natural 2-transitive action of degree 12 and an exceptional 2-transitive action of degree 11.

The group M_{24} is 5-transitive of degree 24 with M_{23} as a one-point stabilizer and M_{22} as a two-point stabilizer; so these latter groups are 4- and 3-transitive, respectively. The point stabilizers in M_{22} are isomorphic to $PSL_3(4)$ in its natural 2-transitive action on the 21 points of the projective plane of order 4 (see Section 2.8). It so happens that we can partition the set Ω of points on which M_{24} acts into two sets of size 12, $\Omega = \Sigma \cup \Gamma$, so that the setwise stabilizer $(M_{24})_{\{\Sigma\}}$ induces the group M_{12} on each of the sets Σ and Γ. Moreover, if α is a point of Σ, then the copy of M_{11} fixing α in the action on Σ induces the 3-transitive action of M_{11}, mentioned above, on the complementary set Γ. The stabilizer in M_{11} of a point $\beta \in \Gamma$ is a copy of $PSL_2(11)$.

The main objective of the present chapter is to construct these groups and their permutation actions. Our approach is concrete and constructive. We build, for each permutation action, an appropriate geometry preserved by the group where these geometries are nested inside one another in the same manner as the groups. Our strategy is to start with the smallest and build successively larger geometries and groups. Initially, the small Mathieu groups (M_{11} and M_{12}) are handled separately from the large Mathieu groups (M_{22}, M_{23} and M_{24}), but at the end we shall explain how M_{12} is embedded inside M_{24} and identify the 3-transitive degree 12 action for M_{11}. (This latter action is also constructed by different means in Example 7.5.2.) However, the first step is to define and develop the type of geometry we use in these constructions.

Exercises

6.1.1 Prove that the Mathieu groups are simple using the fact that $PSL_2(11)$ and $PSL_3(4)$ are both simple. [*Hint:* Use Theorem 7.2B on normal subgroups of multiply transitive groups.]

6.1.2 Show that if G is transitive of prime degree p and $|G| = p \cdot m \cdot k$ where $m > 1$, $m \equiv 1 \bmod p$ and k is a prime with $k < p$ then G is simple. Hence, use the facts that $|M_{23}| = 23 \cdot 40320 \cdot 11$ and $|M_{11}| = 11 \cdot 144 \cdot 5$ to show that these groups are simple.

6.2 Steiner Systems

We have already seen examples of permutation groups as automorphism groups of a structure such as a graph, affine space or projective space (see Sections 2.3, 2.8). Here we define a general class of combinatorial geometries whose automorphism groups have turned out to yield interesting permutation groups.

In an affine or projective space each pair of points is contained in a unique line; it is this "geometric" property which we seek to generalize.

Definition. A *Steiner system* $S = S(\Omega, \mathcal{B})$ is a finite set Ω of *points* together with a set $\mathcal{B}$ of subsets of Ω called *blocks* such that, for some integers k and t, each block in $\mathcal{B}$ has size k, and each subset of Ω of size t lies in exactly one block from $\mathcal{B}$.

We call S an $S(t, k, v)$ Steiner system where $v := |\Omega|$. The parameters are assumed to satisfy $t < k < v$ to eliminate trivial examples.

It is important that this use of the term "block" should not be confused with the earlier use in reference to imprimitive groups. The terminology is too well established to change, but confusion will be minimized in our case since the groups dealt with in this chapter will be multiply transitive, so blocks of imprimitivity will not arise.

An automorphism of a Steiner system $S(\Omega, \mathcal{B})$ is a permutation of Ω which permutes the blocks among themselves. Many interesting permutation groups, not least the Mathieu groups, arise as automorphism groups of Steiner systems. This gives a means of constructing the groups as well as a concrete tool to study the structure of the groups. The study of Steiner systems and other combinatorial geometries is a lively area of combinatorics quite apart from its role in permutation groups. See, for example, Cameron and van Lint (1991), Hughes and Piper (1985), Beth et al. (1993).

The following examples give some idea of the ways in which automorphism groups of Steiner systems arise. The affine and projective groups were introduced in Section 2.8 and the other groups mentioned in the examples are discussed later in Section 7.7.

EXAMPLE 6.2.1. (Affine space as a Steiner system) Take Ω to be the vector space of dimension d over the field $\mathbb{F}_q$ for some prime power q. Take the set $\mathcal{B}$ of blocks to be the affine lines of the space, that is, the translates of 1-dimensional subspaces. Then there are $v = q^d$ points in the space and each block has $k = q$ points on it. Any two distinct points are joined by a unique line so lie together in just one block. Thus we have an $S(2, q, q^d)$ Steiner system. The group $A\Gamma L_d(q)$ (see Section 2.8) is the automorphism group of this Steiner system.

EXAMPLE 6.2.2. (Projective space as a Steiner system) Take Ω to be the set of 1-dimensional subspaces of a vector space of dimension $d + 1$ over the field $\mathbb{F}_q$ for some prime power q. Take the 2-dimensional subspaces as the set $\mathcal{B}$ of blocks. Then there are $v = (q^{d+1} - 1)/(q - 1)$ points and each block contains exactly $k = q + 1$ points. Two points correspond to two 1-dimensional subspaces, so together they span a single 2-dimensional subspace. Thus every pair of distinct points lies in a unique block. Hence the projective space of dimension d is an example of an $S(2, q+1, v)$ Steiner system where $v = (q^{d+1} - 1)/(q - 1)$. The group $P\Gamma L_{d+1}(q)$ (see Section 2.8) is the automorphism group of this Steiner system.

EXAMPLE 6.2.3. In any affine space three distinct points define a plane unless they are collinear. If the field of scalars is $\mathbb{F}_2$ then three points cannot be collinear since lines contain only two points. Therefore the points and planes of $AG_d(2)$ form an $S(3, 4, 2^d)$ Steiner system with the 3-transitive automorphism group $AGL_d(2)$.

EXAMPLE 6.2.4. An *inversive plane* is an $S(3, m + 1, m^2 + 1)$ Steiner system. For each prime power q there is a classical example of an inversive plane with $m = q$ on which $PGL_2(q)$ acts as an automorphism group. If s is odd there is also an inversive plane, with $m = 2^s$, having the Suzuki group $Sz(2^s)$ as a simple 2-transitive automorphism group. See Sect. 7.7 for further details.

EXAMPLE. 6.2.5 A *unital* is an $S(2, m+1, m^3+1)$ Steiner system. If m is an odd prime power then there is a classical unital with 2-transitive automorphism group $PGU_3(m)$. For each odd s there is also a unital with $m = 3^s$ which admits the Ree group $R(3^s)$ as a simple 2-transitive group of automorphisms. See Sect. 7.7 for further details.

EXAMPLE. 6.2.6 The previous examples form infinite families. There are also many examples of Steiner systems which occur in isolation or form part of a small finite collection. For example, there are (up to isomorphism) 16 $S(2, 4, 25)$ Steiner systems with non-trivial automorphism groups [see Kramer, Magliveras and Mathon (1989)]. See also Exercise 6.2.5.

The basic parameters of a Steiner system are the numbers v, k, t and the number $b := |\mathcal{B}|$ of blocks. Given any point α, we can count the number of blocks containing α as follows. We can choose $t-1$ further points from Ω in $\binom{v-1}{t-1}$ ways, and so this is the number of t-subsets which contain α. Similarly, any block (of size k) which contains α has $\binom{k-1}{t-1}$ t-subsets containing α. Since each t-subset lies in a unique block, we conclude that there are exactly $r := \binom{v-1}{t-1}/\binom{k-1}{t-1}$ blocks containing α; in particular, r is independent of the point α. A similar argument shows that more generally, if $1 \le i \le t$, then the number λ_i of blocks which contain a specified i-subset of points is independent of the subset chosen and is given by

$$\lambda_i = \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} = \frac{(v-i)(v-i-1)\cdots(v-t+1)}{(k-i)(k-i-1)\cdots(k-t+1)} \quad \text{for } i = 1, \ldots, t.$$

In the proof of the next theorem we shall need the concept of an *incidence matrix* for a Steiner system $S(\Omega, \mathcal{B})$. This is a matrix whose rows are indexed by the set Ω and whose columns are indexed by $\mathcal{B}$ (in some ordering), and whose (α, B)-th entry is 1 if $\alpha \in B$ and 0 otherwise.

Theorem 6.2A. *Let S be an $S(t, k, v)$ Steiner system with b blocks such that each point lies in exactly r blocks. Then:*
(i) $bk = vr$;
(ii) $r = \dfrac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}$;
(iii) *(Fisher's inequality) $v \le b$ and $k \le r$.*

PROOF. (i) We count, in two ways, the number m of pairs (α, B) such that the point α is contained in the block B. There are b choices for B and then k choices for a point inside; thus $m = bk$. On the other hand, there are v ways to choose α and then r choices for a block containing α; thus $m = vr$. This proves (i)

(ii) This follows at once from the calculations above ($r = \lambda_1$).

(iii) This part requires a more sophisticated argument. Let A be the incidence matrix for S. Then the definition of Steiner system implies that

$$AA^{\mathrm{T}} = \begin{bmatrix} r & 1 & \dots & 1 \\ 1 & r & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & r \end{bmatrix}.$$

The determinant of the $v \times v$ matrix AA^{T} is $(v+r-1)(r-1)^{v-1}$ (see Exercise 6.2.2 below), and this is nonzero because $r \geq 2$. Thus the $v \times b$ matrix A must have rank v. Therefore $v \leq b$, and then (i) shows that $k \leq r$. □

It follows from this theorem that we can calculate b and r from v, k and t, and this explains why these parameters are not mentioned in our notation $S(t, k, v)$. The theorem also shows that there are restrictions on the triples which can appear as the parameters of a Steiner system; more generally, v, k and t must be such that each of the expressions for λ_i is an integer. There seems to be no simple necessary and sufficient condition to characterize the triples (v, k, t) for which a Steiner system exists.

Exercises

6.2.1 Show that the parameters of an $S(t, k, v)$ Steiner system satisfy $v \geq (t+1)(k-t+1)$.

6.2.2 Show that an $n \times n$ matrix of the form

$$\begin{bmatrix} a_1 + c & a_1 & \dots & a_1 \\ a_2 & a_2 + c & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_n & \dots & a_n + c \end{bmatrix}$$

has determinant $c^{n-1}(c + a_1 + \cdots + a_n)$.

6.2.3 Prove the following properties of a Steiner system with parameters $(2, k, v)$:

(i) If $b > v$ then $v \geq k^2$.

(ii) The following are equivalent: (a) $v = k^2$; (b) $r = k+1$; (c) $b = k(k+1)$; (d) if α is a point not in a block B, then there is a unique block which contains α and does not intersect B.

(iii) In the situation of part (ii), the blocks can be partitioned into $k+1$ "parallel classes" each consisting of k blocks such that the blocks in a given parallel class are disjoint. (A Steiner system with this property is called an *affine plane*.)

6.2.4 An $S(2, n+1, n^2+n+1)$ Steiner system is called a *projective plane* of order n.

(i) Suppose that P is a projective plane of order n, and L is a block. Show that if L and all the points on it are removed, then the

resulting system of points and blocks is an affine plane (as in Exercise 6.2.3).

(ii) Conversely, suppose that A is an affine plane of order n. Show that there is a projective plane P of order n and a block L of P such that the removal of L and all its points from P leaves A. Moreover, any two projective planes with this property are isomorphic.

(iii) Show that in a projective plane any two blocks meet in a unique point.

We are concerned here with Steiner systems as geometries on which permutation groups can act. An automorphism group of a Steiner system acts on both the points and the blocks. These two actions are linked in subtle ways as shown in the following theorem.

Theorem 6.2B. *Let $S = S(\Omega, \mathcal{B})$ be a Steiner system and suppose that G is a group of automorphisms of S. Then:*
(i) *G has at least as many orbits on $\mathcal{B}$ as on Ω.*
(ii) *If G acts transitively on both $\mathcal{B}$ and on Ω, then the rank of G acting on $\mathcal{B}$ is at least as great as the rank of G acting on Ω.*

Remark. Part (i) applied with $G = 1$ gives Fisher's Inequality (Theorem 6.2A(iii)).

PROOF. (i) Suppose that $\Omega_1, \Omega_2, \dots, \Omega_s$ are the orbits of G on Ω, and set $n_i := |\Omega_i|$. Similarly, let $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_t$ denote the orbits of G on $\mathcal{B}$. We have to show that $s \leq t$.

Since we are working with orbits, it makes sense to define c_{ik} as the number of points in Ω_i which lie in any given block in $\mathcal{B}_k$, and to define d_{ki} as the number of blocks in $\mathcal{B}_k$ which contain a given point of Ω_i ($i = 1, \dots, s$ and $k = 1, \dots, t$). The point is, these numbers are independent of the particular block or the particular point chosen.

Fix i and j and consider the set

$$T := \{(\alpha, B, \beta) \in \Omega_i \times \mathcal{B} \times \Omega_j \mid \alpha, \beta \in B\}.$$

We count the number of elements of T in two ways. If we first pick $\beta \in \Omega_j$, and then $B \in \mathcal{B}_k$ with $\beta \in B$, and finally $\alpha \in \Omega_i \cap B$, then this gives

$$|T| = \sum_k n_j d_{kj} c_{ik}.$$

Alternatively, if we first pick $\alpha \in \Omega_i$ and $\beta \in \Omega_j$, and then choose the block B containing these points, then (using the definition of λ_i given above) we obtain

$$|T| = \begin{cases} n_i(n_i - 1)\lambda_2 + n_i\lambda_1 & \text{if } i = j \\ n_i n_j \lambda_2 & \text{if } i \neq j \end{cases}.$$

Equating these two expressions for $|T|$ and dividing through by n_j shows that

$$\sum_k c_{ik}d_{kj} = \begin{cases} (n_i - 1)\lambda_2 + \lambda_1 & \text{if } i = j \\ n_i\lambda_2 & \text{if } i \neq j \end{cases}.$$

Defining the matrices $C := [c_{ik}]$ and $D := [d_{kj}]$, this last set of relations can be written:

$$CD = \begin{bmatrix} (n_1 - 1)\lambda_2 + \lambda_1 & n_1\lambda_2 & \cdots & n_1\lambda_2 \\ n_2\lambda_2 & (n_2 - 1)\lambda_2 + \lambda_1 & \cdots & n_2\lambda_2 \\ \vdots & \vdots & \ddots & \vdots \\ n_s\lambda_2 & n_s\lambda_2 & \cdots & (n_s - 1)\lambda_2 +_1 \lambda \end{bmatrix}$$

Now Exercise 6.2.2 shows that $\det(CD) = (\lambda_1 - \lambda_2)^{s-1}(\lambda_1 - \lambda_2 + v\lambda_2)$ because $\sum n_i = v$. Thus CD is nonsingular and so the $s \times t$ matrix C has rank s; hence $s \leq t$ as required.

(ii) Fix $\alpha \in \Omega$ and $B \in \mathcal{B}$, and let m be the number of orbits of G acting on $\Omega \times \mathcal{B}$. Then by the transitivity of G on Ω and $\mathcal{B}$, m is equal to both the number of orbits of G_α on $\mathcal{B}$ and to the number of orbits of $G_{\{B\}}$ on Ω. Now the rank of G acting on Ω equals the number of orbits of G_α acting on Ω, and hence is at most m by part (i). On the other hand the rank of G acting on $\mathcal{B}$ is equal to the number of orbits of $G_{\{B\}}$ acting on $\mathcal{B}$, and again part (i) shows that this is at least m. This proves (ii). □

Exercises

6.2.5 Show that if an $S(2,4,25)$ Steiner system has an automorphism of prime order p then $p = 2$, 3, 5 or 7. The number of fixed points of such an automorphism is: 1 or 5 if $p = 2$; 1 or 4 if $p = 3$; 0 if $p = 5$; and 4 if $p = 7$.

6.2.6 Consider an $S(t,k,v)$ Steiner system and let $B = \{\alpha_1, \ldots, \alpha_k\}$ be a block. For $0 \leq j \leq i \leq k$, let μ_{ij} denote the number of blocks B' for which $B' \cap \{\alpha_1, \ldots, \alpha_i\} = \{\alpha_1, \ldots, \alpha_j\}$. For example, with the usual notation, $\mu_{00} = b$ and $\mu_{11} = r$. The numbers μ_{ij} form what is called the *intersection triangle* of the system.
   (i) Prove that $\mu_{ii} = \binom{v-i}{t-i}/\binom{k-i}{t-i}$ and that $\mu_{ij} = \mu_{i-1,j} - \mu_{i,j-1}$ for all $j < i$.
   (ii) Writing the intersection triangle in the form

$$\begin{array}{ccccccc} & & & \mu_{00} & & & \\ & & \mu_{10} & & \mu_{11} & & \\ & \mu_{20} & & \mu_{21} & & \mu_{22} & \\ \cdots & & \cdots & & \cdots & & \cdots \end{array}$$

the triangle for an $S(5, 6, 12)$ Steiner system is

$$\begin{array}{ccccccccccccc}
 & & & & & & 132 & & & & & & \\
 & & & & & 66 & & 66 & & & & & \\
 & & & & 30 & & 36 & & 30 & & & & \\
 & & & 12 & & 18 & & 18 & & 12 & & & \\
 & & 4 & & 8 & & 10 & & 8 & & 4 & & \\
 & 1 & & 3 & & 5 & & 5 & & 3 & & 1 & \\
1 & & 0 & & 3 & & 2 & & 3 & & 0 & & 1
\end{array}$$

Use this triangle to show that in such a Steiner system the complement of a block is also a block. (In Section 6.4 we shall show that there is a unique Steiner system with these parameters.)

(iii) Construct the intersection triangle for the $S(5, 8, 24)$ Steiner system and use it to show that two blocks of this Steiner system cannot intersect in exactly 1 or 3 points.

6.2.7 The intersection triangle of the previous problem can be extended to any set $X = \{\alpha_1, \ldots, \alpha_m\}$ of points in the Steiner system with $m > k$ if we know the values of μ_{ii} for $i \le m$. Consider an $S(3, 4, 10)$ Steiner system. Construct the intersection triangle corresponding to a set X of five points containing no block. Use the intersection triangle to show that the complement of X also fails to contain a complete block.

Suppose that $S = S(\Omega, \mathcal{B})$ is an $S(t, k, v)$ Steiner system. For any point α of S, we can form a new Steiner system $S_\alpha = S(\Omega', \mathcal{B}'\}$ where $\Omega' := \Omega \setminus \{\alpha\}$ and $\mathcal{B}' := \{B \setminus \{\alpha\} \mid B \in \mathcal{B} \text{ and } \alpha \in B\}$. The Steiner system S_α is called the *contraction* of S at α and is an $S(t-1, k-1, v-1)$ Steiner system. The contraction S_α is also sometimes called the derived or restricted Steiner system. This formation of the contraction of a Steiner system is a basic tool which we shall use frequently in this chapter; it is analogous to working with a point stabilizer in a group. We shall also speak of S as being an *extension* of S_α. While contraction of a Steiner system is always possible, it is rare to find an extension of a given Steiner system. In order to extend an $S(t, k, v)$ Steiner system S, a new set of blocks each with $k + 1$ points must be found. The new set of blocks must have the property that any set of $t + 1$ points of S not contained in a block of S is in exactly one new block. In this chapter construction of extensions of Steiner systems is a major theme, but you should note that the sequences of extensions which we build here are highly exceptional.

The following exercises develop some basic ideas used repeatedly in later sections.

Exercises

6.2.8 An inversive plane was defined in Example 6.2.4 as an $S(3, m + 1, m^2 + 1)$ Steiner system. Show that the contraction of an inversive plane is an affine plane (as defined in Exercise 6.2.3).

6.2.9 Suppose that G is an automorphism group of a Steiner system S and that α is a point of S. Show that G_α is an automorphism group of the contraction S_α.

6.2.10 Suppose that a Steiner system S has an extension S^* obtained by adding the point α and the new set $\mathcal{S}$ of blocks. Show that a group H of automorphisms of S is also a group of automorphisms of S^* if and only if H leaves $\mathcal{S}$ invariant in its induced action on the subsets of the points of S.

6.2.11 Let S be an $S(t, k, v)$ Steiner system and S^* be an extension of S obtained by adding a new point α to each of the blocks of S and adding some new set $\mathcal{S}$ of blocks. Suppose that S is determined uniquely (up to isomorphism) by its parameters and that any two possible choices for the set $\mathcal{S}$ are conjugate under some automorphism of S. Prove that $\mathrm{Aut}(S^*)$ is transitive on the points of S^*, and that $\mathrm{Aut}(S^*)_\alpha$ (as a permutation group acting on the points of S) is the largest subgroup of $\mathrm{Aut}(S)$ which leaves the set $\mathcal{S}$ invariant.

6.3 The Extension of $AG_2(3)$

The Mathieu groups will be constructed by building Steiner systems which have the required groups as their automorphism groups. The first Steiner system to look at is the affine geometry $AG_2(3)$. We have already seen in Example 6.2.1 that, with lines as blocks, this geometry is an $S(2, 3, 9)$ Steiner system. In fact, we shall see that this Steiner system can be extended three times to produce systems with parameters $S(3, 4, 10)$, $S(4, 5, 11)$ and $S(5, 6, 12)$ with the small Mathieu groups as the corresponding automorphism groups. The new blocks to be added at each stage will be subsets of the affine plane $AG_2(3)$, so we shall begin with a detailed study of the geometry of this finite plane.

The affine plane $AG_2(3)$ is the set of nine points in the 2-dimensional vector space over the field $\mathbb{F}_3 = \{0, 1, 2\}$. To simplify notation we shall write ij in place of (i, j) $(i, j \in \{0, 1, 2\})$ for the elements of $AG_2(3)$. Each of the 12 lines of $AG_2(3)$ contains exactly three points, and every pair of points lies on a unique line. We can partition these 12 lines into four classes, each consisting of three parallel lines, namely:

00 01 02	00 10 20	00 11 22	00 12 21
10 11 12	01 11 21	01 12 20	01 10 22
20 21 22	02 12 22	02 10 21	02 11 20

Exercises

6.3.1 Show that in $AG_2(3)$ there are: (i) 72 triangles, (ii) 54 quadrangles (sets of four points with no three collinear), (iii) 4 triangles in each quadrangle, and (iv) 3 quadrangles containing a given triangle.

6.3.2 Show that the automorphism group of $AG_2(3)$ induces S_4 on the set of 4 parallel classes.

6.3.3 Show that every set of five points in $AG_2(3)$ contains at least one quadrangle.

Theorem 6.3A. *Up to isomorphism, $AG_2(3)$ is the unique $S(2,3,9)$ Steiner system.*

PROOF. Consider any $S(2,3,9)$ Steiner system S. In anticipation of the result, we shall refer to its blocks as "lines". We have seen (Exercise 6.2.3 with $k = 3$) that the lines of S can be partitioned into 4 parallel classes. Pick one parallel class and write down its lines as three rows. Rearrange the points in the rows so that the columns form the lines of a second parallel class. Finally, by perhaps interchanging the last two rows we can assume that the diagonal points also form a line of S. Thus we can assume that seven of the 12 lines of S can be displayed as in Fig. 6.1. There are five more lines needed to complete the Steiner system. However, taking any two points not already joined by a line, there is exactly one way to choose the third point on this line. Therefore, there is a unique $S(2,3,9)$ Steiner system. □

We want to extend $AG_2(3)$ to an $S(3,4,10)$ Steiner system (to be called W_{10}) by adding a new point α and defining appropriate new blocks. The Steiner system W_{10} will have $b = 30$ blocks, $r = 12$ blocks containing each point, and each triple of points will be contained in a unique block. As discussed in the last section, the blocks of W_{10} containing α will have the form $\Lambda \cup \{\alpha\}$ where Λ is a line of $AG_2(3)$. These twelve blocks $\Lambda \cup \{\alpha\}$ cover all triples which include α as well as all collinear triples of points of $AG_2(3)$. The remaining blocks must cover the triangles of $AG_2(3)$ once each. The required blocks of W_{10} consist of all sets of four points from $AG_2(3)$ of which no three are collinear (since the collinear triples are already in the blocks $\Lambda \cup \{\alpha\}$). Thus we are looking for a set of $18 = 30 - 12$ quadrangles to cover the 72 triangles of $AG_2(3)$ once each. We shall show that there are exactly three such sets of 18 quadrangles and these three sets partition the set of all 54 quadrangles of $AG_2(3)$.

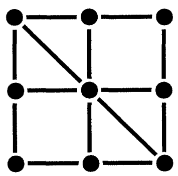


FIGURE 6.1.

We need to make a careful study of the quadrangles of $AG_2(3)$. Since the automorphism group of $AG_2(3)$ is transitive on quadrangles (Exercise 2.8.11), it is sufficient to look at one particular quadrangle, say $\{00, 01, 10, 11\}$. For each quadrangle Ξ there are six lines joining its four points in pairs; we call these the *lines* of the quadrangle. Since each line of $AG_2(3)$ lies in one of the four parallel classes, we see that to each quadrangle Ξ we can associate a pair $\{x, y\}$ of parallel classes such that these are the classes that each contain two of the six lines of Ξ. We shall say that Ξ has *type* $\{x, y\}$.

Exercise

6.3.4 Consider any quadrilateral Ξ of $AG_2(3)$.
(i) Show that there is a unique point δ outside of Ξ which lies on two distinct lines of Ξ. (This point is called the *diagonal point* of the quadrilateral.)
(ii) Show that there is a unique quadrilateral Ξ^* disjoint from Ξ and that Ξ and Ξ^* have the same diagonal point.
(iii) If the parallel classes of $AG_2(3)$ are a, b, c, d and Ξ has type $\{a, b\}$, show that Ξ^* has type $\{c, d\}$.
(iv) If Ξ is a quadrangle of type $\{a, b\}$, and γ is a point outside Ξ such that the only quadrangles contained in $\Xi \cup \{\gamma\}$ are of type $\{a, b\}$ or $\{c, d\}$, show that γ is the diagonal point of Ξ.

The set $\{a, b, c, d\}$ of four parallel classes of $AG_2(3)$ can be partitioned in three different ways into a pair of 2-subsets, namely: $ab \mid cd$, $ac \mid bd$ and $ad \mid bc$. Taking the partition $ab \mid cd$ as an example we can form the set $\mathcal{S}_1$ of all quadrangles of $AG_2(3)$ which either have type $\{a, b\}$ or type $\{c, d\}$. This gives three sets of quadrangles (which we denote $\mathcal{S}_1, \mathcal{S}_2$ and $\mathcal{S}_3$), one for each partition, and each quadrangle belongs to exactly one of these sets. Since the automorphism group of $AG_2(3)$ acts like S_4 on the set of parallel classes (see Exercise 6.3.2), each of these sets contains 18 of the 54 quadrangles of $AG_2(3)$.

Theorem 6.3B. *Each set $\mathcal{S} = \mathcal{S}_i (i = 1, 2, 3)$ has the property:*

(6.1) *each triangle of $AG_2(3)$ is in a unique quadrangle from $\mathcal{S}$.*

Conversely, these are the only sets of 18 quadrangles with this property.

PROOF. We first show that each $\mathcal{S}_i$ has the property (6.1). By symmetry it is enough to consider the case where $\mathcal{S}_i$ corresponds to the partition $ab \mid cd$. Consider any triangle T. The three sides of T are in different parallel classes and so one parallel class, say d, is not represented. When T is completed to a quadrangle by adding a point π, the three lines through π will all lie in different parallel classes. Thus the class d cannot be represented twice by the lines of this quadrangle, and so T is not contained in any quadrangle of type $\{c, d\}$. On the other hand, there is a unique quadrangle of type

$\{a, b\}$ containing T. Indeed we can enumerate the vertices of T as ρ, σ and τ, say, where the line through ρ and σ is in class a, and the line through ρ and τ is in class b. Then the (unique) line of class a through τ and the line of class b through σ intersect at a point π, and $\Xi := \{\sigma, \rho, \tau, \pi\}$ is the unique quadrilateral of type $\{a, b\}$ containing T. As we noted above, no quadrangle containing T has type $\{c, d\}$, so Ξ is the unique quadrilateral in $\mathcal{S}_i$ which contains T. This proves that the sets $\mathcal{S}_i$ have property (6.1).

To prove the converse, let $\mathcal{S}$ be a set of 18 quadrangles satisfying (6.1). For each set $\{\sigma, \rho\}$ of distinct points we define $\mathcal{Q}(\sigma, \tau)$ to be the set of all quadrangles in $AG_2(3)$ which contain these points. In particular, we can enumerate the nine quadrangles in $\mathcal{Q}(00, 01)$ (by their two additional points) as follows:

$$\Xi_1 : 10, 11;\ \Xi_2 : 10, 12;\ \Xi_3 : 10, 21;\ \Xi_4 : 11, 12;\ \Xi_5 : 11, 20;$$

$$\Xi_6 : 12, 22;\ \Xi_7 : 20, 21;\ \Xi_8 : 20, 22;\ \Xi_9 : 21, 22.$$

Since there are six triangles which contain the points 00 and 01 and each quadrangle contains four triangles, condition (6.1) shows that $\mathcal{S}$ must contain exactly three of these quadrangles. It is now straightforward to see that this leaves only three possibilities for $\mathcal{S} \cap \mathcal{Q}(00, 01)$, namely: $\{\Xi_1, \Xi_6, \Xi_7\}$, $\{\Xi_2, \Xi_5, \Xi_9\}$ or $\{\Xi_3, \Xi_4, \Xi_8\}$. Moreover, in each of these cases, $\mathcal{S} \cap \mathcal{Q}(00, 01) \subseteq \mathcal{S}_i$ for some i $(1 \leq i \leq 3)$. Since $AGL_2(3)$ acts 2-transitively on $AG_2(3)$ and leaves the condition (6.1) invariant, this implies the following more general fact: For each set $\{\sigma, \rho\}$ of distinct points there exists i such that $\mathcal{S} \cap \mathcal{Q}(\sigma, \rho) \subseteq \mathcal{S}_i$. It remains to show that i is independent of $\{\sigma, \rho\}$.

Now suppose that $\{\sigma, \rho\}$ and $\{\sigma', \rho'\}$ are both sets of distinct points with $\mathcal{S} \cap \mathcal{Q}(\sigma, \rho) \subseteq \mathcal{S}_i$ and $\mathcal{S} \cap \mathcal{Q}(\sigma', \rho') \subseteq \mathcal{S}_{i'}$; we claim that $i = i'$. Indeed we can choose triangles T and T' such that $\{\sigma, \rho\} \subseteq T$, $\{\sigma', \rho'\} \subseteq T'$ and $|T \cap T'| = 2$. Let Ξ and Ξ' be the quadrangles in $\mathcal{S}$ containing T and T', respectively. Then $\Xi \in \mathcal{S}_i$ and $\Xi' \in \mathcal{S}_{i'}$ while both these quadrangles are contained in $\mathcal{S} \cap \mathcal{Q}(T \cap T') \subseteq \mathcal{S}_j$, say. Hence $i = j = i'$ as required.

This proves that $\mathcal{S} \subseteq \mathcal{S}_i$ for some i, and so the second part of the theorem is proved. □

Corollary 6.3A. *All Steiner systems which are one-point extensions of $AG_2(3)$ are isomorphic.*

PROOF. It follows from the theorem that when we extend $AG_2(3)$ by adding a point α, the 18 blocks which do not contain α can be chosen in just three different ways; namely, as one of the sets $\mathcal{S}_1, \mathcal{S}_2$ or $\mathcal{S}_3$. The automorphism group $AGL_2(3)$ of $AG_2(3)$ induces S_4 on the set of 4 parallel classes (see Exercise 6.3.2), and hence induces S_3 on the set of 3 partitions $\{ab \mid cd,\ ac \mid bd,\ ad \mid bc\}$. Thus $AGL_2(3)$ acts transitively on $\{\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3\}$, and so all the one-point extensions of $AG_2(3)$ are isomorphic. □

Theorem 6.3C. *Up to isomorphism, there is a unique* $S(3,4,10)$ *Steiner system which we shall denote by* W_{10}. *Its automorphism group* $\mathrm{Aut}(W_{10})$ *is 3-transitive on the set of points of* W_{10} *and has order* $10 \cdot 9 \cdot 8 \cdot 2$.

PROOF. Consider an $S(3,4,10)$ Steiner system W and a point α of W. When we contract W at α by removing α and all the blocks not containing it, we end up with an $S(2,3,9)$ Steiner system. By Theorem 6.3A, there is only one such geometry, namely $AG_2(3)$. Hence by Corollary 6.3A, W is determined up to isomorphism and we shall denote it by W_{10}.

If α and β are two points of W_{10}, then the contractions obtained by deleting α and β, respectively, are isomorphic under a mapping ϕ which takes the blocks not containing α (a set $\mathcal{S}_i$ of 18 quadrangles) to the blocks not containing β. We can extend ϕ to all of W_{10} by mapping α to β to obtain an automorphism of W_{10}. This shows that $\mathrm{Aut}(W_{10})$ is transitive. Now the stabilizer of a point in $\mathrm{Aut}(W_{10})$ is isomorphic to the subgroup of $AGL_2(3)$ which fixes one of the sets $\mathcal{S}_i$, say $\mathcal{S}_1$. This latter subgroup is just the stabilizer of the partition $ab \mid cd$ of the four parallel classes, and so it is a subgroup of index 3 in $AGL_2(3)$. Since the order of $AGL_2(3)$ is $9 \cdot 8 \cdot 6$, we have $|(\mathrm{Aut}(W_{10}))_\alpha| = 9 \cdot 8 \cdot 2$ and $|\mathrm{Aut}(W_{10})| = 10 \cdot 9 \cdot 8 \cdot 2$. The stabilizer in $AGL_2(3)$ of the partition $ab \mid cd$ is 2-transitive on the points of $AG_2(3)$ (Exercise 6.3.5 below), so $\mathrm{Aut}(W_{10})$ is 3-transitive as asserted. □

Exercise

6.3.5 Let H be the stabilizer in $AGL_2(3)$ of the partition $ab \mid cd$. Show that the stabilizer $H_{\{a,b\}}$ in H of the pair $\{a,b\}$ has index 2 and is sharply 2-transitive on the points of $AG_2(3)$. [*Hint:* The group T of translations in $AGL_2(3)$ fixes all parallel classes.]

The group $\mathrm{Aut}(W_{10})$ has a subgroup of index 2 which is called M_{10} (although, strictly, M_{10} is not a Mathieu group). The group M_{10} is a sharply 3-transitive group which is isomorphic to a proper subgroup of $PGL_2(9)$ containing $PSL_2(9)$. The point stabilizer $(M_{10})_\alpha$ is the stabilizer in $AGL_2(3)$ of all three sets $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$. The group M_{10} will appear later as the pointwise stabilizer in M_{12} of a pair of points.

6.4 The Mathieu Groups M_{11} and M_{12}

In this section we shall extend the Steiner system W_{10} to an $S(4,5,11)$ Steiner system which we denote W_{11}, and then extend again to an $S(5,6,12)$ Steiner system called W_{12}. These W_i, as well as the Steiner systems associated with the large Mathieu groups, are called *Witt geometries*. The methods used will build on the previous section but, in fact, all of the hard work has already been done there.

First assume that we have an $S(4,5,11)$ Steiner system W and select two points α, β in W. Then the contractions of W at α and β, respectively, are both $S(3,4,10)$ Steiner systems, so by Theorem 6.3C they are isomorphic, and each is an extension of $AG_2(3)$ of the sort constructed in Section 6.3. We may assume that the set of points in W is just the set of points in $AG_2(3)$ together with α and β. Then the blocks of W containing α and β are of the following forms: $\Lambda \cup \{\alpha, \beta\}$ where Λ is a line of $AG_2(3)$; $\Xi \cup \{\alpha\}$ where Ξ is a quadrangle in $\mathcal{S}_1$; and $\Xi \cup \{\beta\}$ where Ξ is a quadrangle in $\mathcal{S}_2$ (where $\mathcal{S}_1$ and $\mathcal{S}_2$ are sets of quadrangles of the type defined in the last section).

It remains to describe the set of those blocks of W which contain neither α nor β (and so are contained in $AG_2(3)$). First recall that any set of five points in $AG_2(3)$ contains a quadrangle (see Exercise 6.3.3), so each of the remaining blocks must contain a quadrangle from $\mathcal{S}_3$. On the other hand, since each set of four points lies in exactly one block, none of these blocks contains a quadrangle from $\mathcal{S}_1$ or $\mathcal{S}_2$, and so Exercise 6.3.4 (iv) shows that each of the blocks of W disjoint from $\{\alpha, \beta\}$ has the form $\Xi \cup \{\delta\}$ where $\Xi \in \mathcal{S}_3$ and δ is the diagonal point of Ξ.

Below we shall show how to reverse this argument to prove the existence of an $S(4,5,11)$ Steiner system.

Theorem 6.4A. *Up to isomorphism there is a unique $S(4,5,11)$ Steiner system which we shall denote by W_{11}, and write $M_{11} := \mathrm{Aut}(W_{11})$. The group M_{11} is sharply 4-transitive on the set of points of W_{11} and has order* $11 \cdot 10 \cdot 9 \cdot 8$.

PROOF. We begin by constructing an $S(4,5,11)$ Steiner system W using the observations made above. Let $\Omega := AG_2(3) \cup \{\alpha, \beta\}$ (where α and β are new points not in $AG_2(3)$) be the set of points of W. Define the set $\mathcal{B}$ of blocks to consist of all sets of the form:

(i) $\Lambda \cup \{\alpha, \beta\}$ where Λ is a line of $AG_2(3)$;
(ii) $\Xi \cup \{\alpha\}$ where $\Xi \in \mathcal{S}_1$;
(iii) $\Xi \cup \{\beta\}$ where $\Xi \in \mathcal{S}_2$; or
(iv) $\Xi \cup \{\delta\}$ where $\Xi \in \mathcal{S}_3$ and δ is the diagonal point of Ξ.

In particular, there are exactly 18 blocks of each of the types (ii)–(iv), and 12 of type (i), so $|\mathcal{B}| = 66$.

We must show that $\mathcal{B}$ is a set of blocks for an $S(4,5,11)$ Steiner system; that is, that each set of four points from W lies in exactly one block. Since $|\mathcal{B}| = \binom{11}{4}/\binom{5}{4}$, it is enough to show that each set of four points is in at least one block. It is clear that any set of four points of W which includes α or β lies in a block from $\mathcal{B}$, and also that any quadrangle in $AG_2(3)$ lies in a block. Thus it remains to show that when U is a set of four points in $AG(3,2)$ containing a line Λ, then U also lies in a block from $\mathcal{B}$ (necessarily of type (iv)). Without loss in generality, assume that $\mathcal{S}_3$ corresponds to the partition $ab \mid cd$ and that Λ lies in parallel class a. If π is the point of U

not on Λ, then we choose $\rho \notin U$ such that the line Λ' through π and ρ is in parallel class b; note that $\Lambda' \subseteq U \cup \{\rho\}$. Finally, let δ be the intersection of Λ and Λ' and let Ξ be the complement of $\{\delta\}$ in $U \cup \{\rho\}$. Then Ξ is a quadrangle of type $\{c, d\}$ with diagonal point γ, and so $U \cup \{\delta\} = \Xi \cup \{\gamma\}$ is a block of type (iv) containing U. Thus $W = S(\Omega, \mathcal{B})$ is an $S(4,5,11)$ Steiner system as asserted.

The uniqueness of an $S(4,5,11)$ Steiner system and the transitivity of its automorphism group now follows as in the proof of Theorem 6.3C and Exercise 6.2.10. We call this Steiner system W_{11} and define $M_{11} := \mathrm{Aut}(W_{11})$. Finally the subgroup $(M_{11})_{\alpha\beta}$ leaves invariant each of the sets $\mathcal{S}_1$ and $\mathcal{S}_2$, and hence also $\mathcal{S}_3$. Thus $(M_{11})_{\alpha\beta}$ has index 6 in $AGL_2(3)$ and so has order $9 \cdot 8$ and is sharply 2-transitive (Exercise 6.3.4). Therefore M_{11} is sharply 4-transitive with order $11 \cdot 10 \cdot 9 \cdot 8$. □

So far we have constructed two successive extensions of the affine plane $AG_2(3)$. We can make one more extension by adding a further point. Before constructing this system we examine what properties it must have.

Our analysis of $AG_2(3)$ told us that there are three sets $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ of quadrangles each of which covers the triangles of $AG_2(3)$ exactly once. For each of the sets $\mathcal{S}_i$, we construct the set $\mathcal{C}_i$ consisting of subsets of $AG_2(3)$ of the form $\Xi \cup \{\delta\}$ where $\Xi \in \mathcal{S}_i$ and δ is the diagonal point of Ξ. Now suppose that W is an $S(5,6,12)$ Steiner system containing points α, β and γ. Since an $S(4,5,11)$ Steiner system is unique up to isomorphism, each of the one-point contractions of W by α, β and γ, respectively, can be constructed as in Theorem 6.4A using the sets $\mathcal{S}_i$ and $\mathcal{C}_i$. Thus, we can assume that the set Ω of points of W is $AG_2(3) \cup \{\alpha, \beta, \gamma\}$, and that the blocks which contain at least one of α, β and γ have the form:

(i) $\Lambda \cup \{\alpha, \beta, \gamma\}$ where Λ is a line of $AG_2(3)$;
(ii) $\Xi \cup \{\beta, \gamma\}$ where Ξ is a quadrangle in $\mathcal{S}_1$;
(iii) $\Xi \cup \{\alpha, \gamma\}$ where Ξ is a quadrangle in $\mathcal{S}_2$;
(iv) $\Xi \cup \{\alpha, \beta\}$ where Ξ is a quadrangle in $\mathcal{S}_3$;
(v) $R \cup \{\alpha\}$ where R is in $\mathcal{C}_1$;
(vi) $R \cup \{\beta\}$ where R is in $\mathcal{C}_2$; or
(vii) $R \cup \{\gamma\}$ where R is in $\mathcal{C}_3$.

The blocks disjoint from $\{\alpha, \beta, \gamma\}$ cannot contain any of the five element subsets in the $\mathcal{C}_i$, and so do not contain a quadrangle with its diagonal point. A simple argument shows that this means that all blocks disjoint from $\{\alpha, \beta, \gamma\}$ are of the form:

(viii) a union of two distinct parallel lines in $AG_2(3)$.

We note that there are 12 sets listed in (i), 18 of each of the types (ii)–(vii), and 12 of type (viii). Thus the set $\mathcal{B}$ of all these blocks has size $|\mathcal{B}| = 132$.

Theorem 6.3B. *Up to isomorphism, there is a unique* $S(5,6,12)$ *Steiner system which we call* W_{12}. *The automorphism group* $M_{12} := \mathrm{Aut}(W_{12})$ *has order* $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ *and is sharply 5-transitive on the points of* W_{12}.

PROOF. The argument is similar to those already used to construct W_{10} and W_{11} and their automorphism groups. We have shown that there is at most one way to extend W_{11} to an $S(5,6,12)$ Steiner system W_{12}, and the verification that (i)–(viii) do indeed define a set of blocks for an $S(5,6,12)$ Steiner system follows that given in the proof of Theorem 6.3A. The first part of our theorem then follows. Now the affine group $AGL_2(3)$ permutes the new blocks of type (viii) in a single orbit, so $(M_{12})_\gamma$ is all of M_{11}. Then the transitivity of the automorphism group M_{12} of W_{12} is immediate by the uniqueness of W_{11} and the fact that $AGL_2(3)$ induces S_3 on both $\{\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3\}$ and on $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$. Finally, the sharp 5-transitivity of M_{12} (and hence the order) follows from the sharp 4-transitivity of M_{11}. □

Exercises

6.4.1 Show that $\mathrm{Aut}(W_{10})$ has a normal subgroup of index 2 isomorphic to S_6.

6.4.2 Show that the stabilizer M_{10} of 2 points in M_{12} has index 2 in $\mathrm{Aut}(W_{10})$.

6.4.3 Let B be a block of W_{12}. Show
- (i) The complement B' of B is also a block. [*Hint:* Use Exercise 6.2.6.]
- (ii) The setwise stabilizer of B in W_{12} induces S_6 on B.
- (iii) An involution in W_{12} which fixes four points of B acts as the product of three 2-cycles on B'. (This exhibits the outer automorphism of S_6; see Section 8.2.)

6.5 The Geometry of $PG_2(4)$

We shall now turn to the construction of the large Mathieu groups. In this case, instead of starting from $AG_2(3)$, we begin with the projective plane $PG_2(4)$.

A finite projective plane is, by definition, an $S(2, n+1, n^2+n+1)$ Steiner system. Exercise 6.2.3 shows that not only are any two points of a projective plane in a unique block, but any two blocks meet in a unique point. It is this property which makes these finite planes similar to the classical (infinite) projective plane. In this section, we shall make a detailed study of the projective plane of order $n = 4$. This is a Steiner system with 21 points and 21 blocks which we shall refer to as lines. We shall establish in Theorem 6.6A that there is only one projective plane of order 4 so it will suffice to work with a concrete representation using coordinates.

In coordinate form, we represent the points of $PG_2(4)$ by nonzero vectors (x, y, z) of dimension 3 over the field $\mathbb{F}_4$ of four elements. Two vectors denote the same (projective) point exactly when they are scalar multiples of one another. In other words, the points of $PG_2(4)$ are identified with the lines through the origin in the vector space. We can give a standard list of representations of the points by: $(0, 0, 1)$, $(0, 1, v)$ and $(1, u, v)$ where u and v run over $\mathbb{F}_4$. Every point is represented by exactly one of these vectors. The lines (= blocks) of $PG_2(4)$ are represented in a similar manner (up to nonzero scalar multiples) and are written $[a, b, c]$ with $a, b, c \in \mathbb{F}_4$ not all zero. A point (x, y, z) lies on the line $[a, b, c]$ if and only if $ax + by + cz = 0$.

More generally, we can define $PG_n(F)$ over any field (or division ring) F, where the "points" are the 1-dimensional subspaces in the $(n + 1)$-dimensional space over F and the "lines" are the 2-dimensional subspaces. A point π is on a line Λ when $\pi \subseteq \Lambda$. Refer to Section 2.8 for further details.

Exercises

6.5.1 Consider the triangle in $PG_2(4)$ with vertices (1,0,0), (0,1,0) and (0,0,1). Show that the point (x, y, z) lies on one of the sides of this triangle if and only if at least one of x, y, z is non-zero. (The sides of the triangle are just the lines going through pairs of vertices.)

6.5.2 Let F be a field and K be a subfield. Show that $PG_2(K)$ can be embedded inside $PG_2(F)$ as a subset of the points and of the lines.

6.5.3 Show that there are exactly five points in $PG_2(4)$ which lie on the conic $X^2 + YZ = 0$; that is, points (x, y, z) such that $x^2 + yz = 0$. (Note that this makes sense only because the polynomial is homogeneous. The homogeneity ensures that two representations of the same point both satisfy the condition or neither does.) Show that no three of these points are collinear. In fact, we can add the point (1,0,0) and the resulting set of six points still has no collinear triples. (Such a set is called a *hyperoval*.)

The group $PGL_3(4)$ was defined in Section 2.8; here we review the construction. It is the group induced by the group of the 3×3 invertible matrices M acting by matrix multiplication on the points and lines of $PG_2(4)$ according to:

$$(x, y, z) \mapsto (x, y, z)M \quad \text{and} \quad [a, b, c] \mapsto [a, b, c](M^{-1})^{\mathrm{T}}.$$

A straightforward calculation shows that permutations defined by M on the sets of points and lines constitute an automorphism of $PG_2(4)$, and that M induces the trivial automorphism if and only if it is a scalar matrix. Thus $PGL_3(4) = GL_3(4)/K$ where K is the subgroup of scalar matrices in $GL_3(4)$. Note that K is isomorphic to the multiplicative group of units of $\mathbb{F}_4$, so it is cyclic of order 3.

The general linear group $GL_3(4)$ has a subgroup $SL_3(4)$ formed by the matrices of determinant 1. Since we are working over $\mathbb{F}_4$ and $SL_3(4)$ is the kernel of the mapping $M \mapsto \det M$, therefore $SL_3(4)$ has index 3 in $GL_3(4)$ and all scalar matrices lie in $SL_3(4)$. Thus the group $PSL_3(4)$ induced by $SL_3(4)$ on the projective plane has index 3 in $PGL_3(4)$ and order $20,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$.

Each field automorphism σ of $\mathbb{F}_4$ induces another type of automorphism g_σ of $PG_2(4)$ defined by

$$(x, y, z) \mapsto (x^\sigma, y^\sigma, z^\sigma) \quad \text{and} \quad [a, b, c] \mapsto [a^\sigma, b^\sigma, c^\sigma].$$

The group generated by $PGL_3(4)$ and the automorphisms g_σ ($\sigma \in \mathrm{Aut}(\mathbb{F}_4)$) is the full automorphism group of the projective plane $PG_2(4)$; it is denoted $P\Gamma L_3(4)$. Since $\mathrm{Aut}(\mathbb{F}_4)$ has order 2 (the only nontrivial automorphism maps $x \mapsto x^2$), the quotient group $P\Gamma L_3(4)/PGL_3(4)$ has order 2. We denote by $P\Sigma L_3(4)$ the subgroup of $P\Gamma L_3(4)$ generated by $PSL_3(4)$ and the field automorphisms, and again we have $P\Sigma L_3(4)/PSL_3(4)$ of order 2, while $P\Gamma L(3,4)/P\Sigma L_3(4)$ has order 3.

Exercise

6.5.4 Let Π and Λ denote the sets of 21 points and 21 lines, respectively, of $PG_2(4)$. Define a mapping φ on $\Pi \cup \Lambda$ which interchanges the points and lines by $\varphi : (x, y, z) \leftrightarrow [x, y, z]$.
  (i) Show that φ preserves incidence.
  (ii) Let C be the set of permutations $\Pi \cup \Lambda$ which preserve incidence and either leave Π and Λ invariant or interchange Π and Λ. Show that C is the subgroup of $Sym(\Pi \cup \Lambda)$ generated by φ and all permutations induced by $P\Gamma L_3(4)$. (In fact, $C \cong \mathrm{Aut}(PSL_3(4))$).

In the rest of this section we shall write $G := PGL_3(4)$ and $S := PSL_3(4)$. By an ordered quadrangle we shall mean an ordered set of four points such that no three are collinear. For any field K, the group $PGL_3(K)$ acts regularly on the set of ordered quadrangles of the projective plane $PG_2(K)$. This fact is the case $d = 3$ of Exercise 2.8.19 and is sometimes referred to as the "Fundamental Theorem of Projective Geometry". For easy reference, we shall record the special case of interest in a theorem.

Theorem 6.5A. *$PGL_3(4)$ acts regularly on the set of ordered quadrangles of $PG_2(4)$.*

PROOF. See Exercise 2.8.19. □

One consequence of Theorem 6.5A is that all quadrangles in $PG_2(4)$ are isomorphic to the standard one: $\Xi = \{(1,0,0), (0,1,0), (0,0,1), (1,1,1)\}$. The six sides of Ξ meet in pairs in the three points (0,1,1), (1,0,1) and (1,1,0) called the *diagonal points* of the quadrangle. In $PG_2(4)$ it happens that these three diagonal points are collinear, lying on the line [1,1,1]. Thus

the quadrangle Ξ together with its three diagonal points defines a set of seven points and seven lines, namely:

$$(1,0,0),(0,1,0),(0,0,1),(1,1,1),(0,1,1),(1,0,1),(1,1,0) \text{ and}$$
$$[1,0,0],[0,1,0],[0,0,1],[1,1,1],[0,1,1],[1,0,1],[1,1,0].$$

These lines and points form a projective plane which is essentially $PG_2(2)$. Each of the points lies on three lines and each line contains exactly three of the points. Moreover, two points of the set are joined by one of the lines and every two lines meet at a point of the set. (You are urged to draw a diagram.) This configuration is called a *Fano subplane*. By Theorem 6.5A every quadrangle in $PG_2(4)$ defines a unique Fano subplane by adding its three diagonal points. The name Fano subplane specifically denotes the projective plane with seven points. In the context under consideration such a subplane is also a *Baer* subplane (a subplane of order m in a projective plane of order m^2), and some authors refer to these planes by this name. It should also be noted that the phenomenon of collinear diagonal points which holds in $PG_2(4)$ depends on the fact that the underlying field has characteristic 2.

Exercises

6.5.5 Show that each line of $PG_2(4)$ meets a given Fano subplane in either 1 or 3 points. What similar statement can you make about the points of $PG_2(4)$ and the lines of a Fano subplane?

6.5.6 Show that if P is a set of seven points of $PG_2(4)$ with the property that every line of $PG_2(4)$ meets P in 1 or 3 points, then P is a Fano subplane.

Returning to the quadrangle Ξ, we shall construct a different type of subset containing Ξ. As we saw above, there are six lines joining pairs of points of Ξ, and each of these lines contains one of the diagonal points. Since each line of $PG_2(4)$ has five points, there are 12 points on the lines of Ξ which are not in the Fano subplane defined by Ξ. These 12 points together with the points of the Fano subplane make a total of 19 points. Therefore there are exactly two points of $PG_2(4)$ (namely, $(1,\omega,\omega^2)$ and $(1,\omega^2,\omega)$ where $\omega \in \mathbb{F}_4$ satisfies $\omega^2+\omega+1=0$) which are not on any line of the Fano subplane of Ξ. The set formed by Ξ and these two points is called a *hyperoval*. It follows from Theorem 6.5A that each quadrangle is contained in a unique hyperoval.

Exercises

6.5.7 Show that the two points added to a quadrangle Ξ to make a hyperoval are on the line joining the diagonal points.

6.5.8 Show that $PG_2(4)$ has 168 hyperovals and 360 Fano subplanes.

6.5.9 Show that a set of six points of $PG_2(4)$ is a hyperoval if and only if it does not contain three collinear points.

6.5.10 Show that each line of $PG_2(4)$ meets a given hyperoval in 0 or 2 points.

6.5.11 Show that a nontrivial automorphism of a projective plane which fixes every point of some line has at most one fixed point not on that line.

6.5.12 Show that any nontrivial element of $PGL_3(4)$ which fixes all points in some quadrangle Ξ has order 2, and that it induces a 2-cycle on the hyperoval of Ξ.

6.5.13 Show that if Δ is a hyperoval in $PG_2(4)$ then
- (i) $PGL_3(4)_{\{\Delta\}}$ acts faithfully on the six points of Δ.
- (ii) $PGL_3(4)_{\{\Delta\}} = PSL_3(4)_{\{\Delta\}}$ and induces A_6 on Δ. [*Hint:* Use Theorem 6.5A and the fact that A_6 is the only sharply 4-transitive subgroup of S_6.]
- (iii) $P\Gamma L_3(4)_{\{\Delta\}} = P\Sigma L_3(4)_{\{\Delta\}}$ and induces S_6 on Δ.

6.5.14 Consider a hyperoval Δ in $PG_2(4)$.
- (i) Show that exactly six lines of $PG_2(4)$ are disjoint from Δ.
- (ii) Show that $PGL_3(4)$ induces S_6 on these 6 lines.
- (iii) Use (ii) to show that S_6 has an outer automorphism.
- (iv) Show that this automorphism also induces an outer automorphism of A_6.

The group $G = PGL_3(4)$ is transitive on quadrangles and each quadrangle is contained in a unique hyperoval and a unique Fano subplane. Hence G is transitive on both the set of hyperovals and the set of Fano subplanes. The situation for the subgroup $S = PSL_3(4)$ is somewhat different. We have $S_{\{\Delta\}} = G_{\{\Delta\}}$ for each hyperoval Δ (Exercise 6.5.13), and S has index 3 in G, so S permutes the set of hyperovals in three orbits of equal size. What about the Fano subplanes? Each Fano subplane Φ is a copy of $PG_2(2)$. The group $PGL_3(2)$ acts regularly on the set of quadrangles of $PG_2(2)$ (Exercise 2.8.19). Note that since the underlying field only has two elements, $PGL_3(2) = PSL_3(2)$. Since any automorphism of Φ which fixes a quadrangle pointwise must be the identity, this shows that $\mathrm{Aut}(\Phi) \cong PSL(3,2)$. Now $PSL_3(2)$ can be identified with the subgroup of S consisting of elements induced by 3×3 matrices over $\mathbb{F}_2$. Thus, the stabilizer $S_{\{\Phi\}}$ of Φ induces the full automorphism group of this plane. Since $G_{\{\Phi\}}$ acts faithfully on Φ, it follows that $G_{\{\Phi\}} = S_{\{\Phi\}}$. Hence S permutes the set of Fano subplanes in three orbits.

Theorem 6.5B.
- (i) *$PSL_3(4)$ acting on the set of 168 hyperovals of $PG_2(4)$ has three orbits, each consisting of 56 hyperovals.*
- (ii) *$PSL_3(4)$ acting on the set of 360 Fano subplanes of $PG_2(4)$ has three orbits, each consisting of 120 subplanes.*
- (iii) *If Δ_1 and Δ_2 are hyperovals, each with four points in common with a particular Fano subplane Φ then Δ_1 and Δ_2 are in the same orbit under $PSL_3(4)$.*

(iv) $P\Gamma L_3(4)$ *induces a cyclic permutation on the orbits of hyperovals of* $PSL_3(4)$, *and the stabilizer is of any orbit is* $PSL_3(4)$.

PROOF. For (i) and (ii), the only point not covered in the preceding discussion is the counting of the hyperovals and Fano subplanes. This is straightforward since each hyperoval and each Fano subplane is uniquely specified by any of its quadrangles (see Exercise 6.5.8).

To prove (iii) we note that, for $i = 1, 2$, the set $\Delta_i \cap \Phi$ is a quadrangle in Φ and determines the hyperoval Δ_i. Since $S_{\{\Phi\}}$ induces $PGL_3(2)$ on Φ and so is transitive on the quadrangles of Φ, some element $x \in S_{\{\Phi\}}$ maps $\Delta_1 \cap \Phi$ to $\Delta_2 \cap \Phi$. Then $\Delta_1 = \Delta_2$, and so the two hyperovals lie in the same $PSL_4(3)$-orbit.

Part (iv) follows from the fact that the quotient group $P\Gamma L_3(4)/PSL_3(4)$ is cyclic of order 6. □

Theorem 6.5B(iii) shows that the hyperovals which have a quadrangle in common with some Fano subplane from a particular $PSL_3(4)$-orbit of Fano subplanes all lie in a single $PSL_3(4)$-orbit. Therefore we can label the $PSL_3(4)$-orbits $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ of hyperovals and the $PSL_3(4)$-orbits $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ of Fano subplanes such that, if $\Delta \in \mathcal{H}_i$ and $\Phi \in \mathcal{F}_j$, then $|\Delta \cap \Phi| \leq 3$ if and only if $i \neq j$. This correspondence will be useful in constructing the Steiner systems of the next section.

6.6 The Extension of $PG_2(4)$ and the Group M_{22}

In this section we construct an $S(3, 6, 22)$ Steiner system which is an extension of the projective plane $PG_2(4)$. The construction is similar to that of Sections 6.3 and 6.4. The first step is to show that the projective plane $PG_2(4)$ is determined uniquely by its parameters.

Theorem 6.6A. $PG_2(4)$ *is the only* $S(2, 5, 21)$ *Steiner system.*

PROOF. If we remove a line and all its points from an $S(2, 5, 21)$ Steiner system, we get an affine plane A with parameters $S(2, 4, 16)$. Moreover it is enough to show that there is a unique $S(2, 4, 16)$ Steiner system (Exercise 6.2.4). So let A be any $S(2, 4, 16)$ Steiner system and note that the 20 lines of A are divided into five parallel classes of which we distinguish two as $\{\Gamma_1, \dots, \Gamma_4\}$ and $\{\Lambda_1, \dots, \Lambda_4\}$. The other 12 lines of A will be denoted $\Delta_1, \dots, \Delta_{12}$. For $j = 1, \dots, 12$ and $i, k = 1, \dots, 4$ we define $t_{ij} := k$ if the point of intersection of Λ_k and Γ_i lies on Δ_j. Then, for each j, the list $t_{1j}, t_{2j}, t_{3j}, t_{4j}$ is a permutation of 1,2,3,4 and so each column of the 4×12 matrix $T := [t_{ij}]$ contains each of the entries 1,2,3,4 exactly once. Moreover, T does not contain a minor of the form $\left[\begin{smallmatrix} a & a \\ b & b \end{smallmatrix}\right]$ since this would correspond to two points being joined by two different lines. Thus, without loss in generality, we can assume that we have labelled the lines in the

parallel classes and the lines in the list $\Delta_1, \ldots, \Delta_{12}$ so that part of the matrix T looks like:

$$\begin{bmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 & 4 & 4 & 4 \\ 2 & 3 & 4 & 1 & 3 & 4 & 1 & 2 & 4 & 1 & 2 & 3 \\ 3 & & & & & & & & & & & \\ 4 & & & & & & & & & & & \end{bmatrix}.$$

To finish the proof it is enough to show that there is only one way to complete the matrix T with the properties noted above. We leave this as a simple exercise. □

We now want to show that the projective plane $PG_2(4)$ can be extended to an $S(3, 6, 22)$ Steiner system W_{22} by adding a new point α. Some of the blocks of W_{22} will be obtained by adjoining α to each of the lines of $PG_2(4)$. In addition we must define some new blocks consisting of six points from $PG_2(4)$. The new Steiner system will have the property that every triple of points in W_{22} lies in a unique block. The triples which include α lie in blocks of the form $\Lambda \cup \{a\}$ where Λ is a line of $PG_2(4)$. These blocks also cover the triples of collinear points in $PG_2(4)$. Thus the new blocks must be defined in such a way that they exactly cover the triangles (triples of noncollinear points) of $PG_2(4)$. Recall that we showed at the end of Section 6.5, that the group $PSL_3(4)$ has three orbits on hyperovals. The following theorem says that each of the $PSL_3(4)$-orbits of hyperovals has this property so an extension of $PG_2(4)$ does exist.

Theorem 6.6B. *Let $\mathcal{H}_i$ be one of the three S-orbits of hyperovals in $PG_2(4)$ where $S := PSL_3(4)$. Then every triangle of $PG_2(4)$ is contained in a unique hyperoval of $\mathcal{H}_i$.*

PROOF. First we observe that S is transitive on the set of ordered triangles of $PG_2(4)$. Indeed, for any triangle from $PG_2(4)$, the homogeneous coordinates of the three points are linearly independent vectors, and so there is a matrix M mapping these three vectors to the vectors (1,0,0), (0,1,0), (0,0,1) representing the vertices of the "standard triangle". Now, if we define N as the diagonal matrix $\mathrm{diag}(1, 1, \det(M)^{-1})$, then N maps each of the latter vectors into a scalar multiple of itself. Thus MN induces a mapping of the given triangle onto the standard triangle and $\det(MN) = 1$. This shows that S is transitive on the set of triangles. Since S is also transitive on $\mathcal{H}_i$, there is a number m such that each triangle is contained in exactly m hyperovals from $\mathcal{H}_i$ (see Exercise 6.6.1). Consider the set $\mathcal{K}$ of quadruples of the form $(\rho, \sigma, \tau, \Delta)$ where $\{\rho, \sigma, \tau\}$ is a triangle and $\{\rho, \sigma, \tau\} \subset \Delta \in \mathcal{H}_i$. If we count $|\mathcal{K}|$ in two ways we find that $21 \cdot 20 \cdot 16 \cdot m = 56 \cdot 6 \cdot 5 \cdot 4$. Hence $m = 1$ and $\mathcal{H}_i$ covers each triangle exactly once as asserted. □

Exercise

6.6.1 Let G be a group acting on a finite set Ω and suppose that $\mathcal{S}_1 \subseteq \Omega^{\{r\}}$ and $\mathcal{S}_2 \subseteq \Omega^{\{s\}}$ with $r \leq s$. If G acts transitively on both $\mathcal{S}_1$ and $\mathcal{S}_2$, show that there exist integers m and n such that each r-subset in $\mathcal{S}_1$ is contained in exactly m s-subsets from $\mathcal{S}_2$, and that each s-subset in $\mathcal{S}_2$ contains exactly n r-subsets from $\mathcal{S}_1$.

We now turn to the uniqueness of the $S(3,6,22)$ Steiner system. Let W be an $S(3,6,22)$ Steiner system. The contraction of W at a point is an $S(2,5,21)$ Steiner system, and so is isomorphic to $PG_2(4)$ (Theorem 6.6A). Thus, without loss in generality, we may assume that W is an extension of $PG_2(4)$ by a point α. Then the blocks of W containing α are of the form $\Lambda \cup \{\alpha\}$ where Λ is a line of $PG_2(4)$, and these blocks contain all triples of collinear points from $PG_2(4)$. Therefore the blocks of W not containing α are sets consisting of six points of $PG_2(4)$ in which no three are collinear; thus they are hyperovals (see Exercise 6.5.9). We want to show that the set $\mathcal{H}$ of blocks of W not containing α is in fact one of the $PSL_3(4)$-orbits of hyperovals. With this in mind we collect some further detailed information about hyperovals in $PG_2(4)$.

Theorem 6.6C.

(i) *Each pair of points of $PG_2(4)$ is in 12 hyperovals in $PG_2(4)$.*

(ii) *Each triangle of points of $PG_2(4)$ is in three hyperovals, one from each $PSL_3(4)$-orbit $\mathcal{H}_i$.*

(iii) *For any hyperoval Δ and two points $\rho, \sigma \in \Delta$, there are three hyperovals in $PG_2(4)$ whose intersection with Δ is exactly $\{\rho, \sigma\}$.*

PROOF. (i) Let ρ and σ be distinct points of $PG_2(4)$. There are $\frac{16\cdot 9}{2}$ ways to complete $\{\rho, \sigma\}$ to a quadrangle, and each of these quadrangles lies in a unique hyperoval (see Section 6.5). On the other hand, each hyperoval containing $\{\rho, \sigma\}$ is counted $\frac{4\cdot 3}{2}$ times in this process. Thus there are $\frac{16\cdot 9}{4\cdot 3} = 12$ hyperovals containing the pair $\{\rho, \sigma\}$.

(ii) A counting argument similar to (i) shows that each triangle lies in three hyperovals. The proof that it lies in one hyperoval from each of the $PSL_3(4)$-orbits follows from Exercise 6.6.1 and the fact that, for each orbit $\mathcal{H}_i$, *some* triangle lies in a hyperoval from $\mathcal{H}_i$.

(iii) Consider a hyperoval Δ and two points $\rho, \sigma \in \Delta$. By (ii) exactly 12 hyperovals contain ρ and σ. On the other hand there are four ways to complete $\{\rho, \sigma\}$ to a triangle in Δ, and (ii) shows that each of these triangles lies in two hyperovals apart from Δ. Since two hyperovals can intersect in at most three points, there are exactly $11 - 4 \cdot 2 = 3$ hyperovals which intersect Δ in exactly $\{\rho, \sigma\}$. □

We are now in a position to establish the uniqueness of the $S(3,6,22)$ Steiner system.

Theorem 6.6D. *Up to isomorphism, there is a unique $S(3,6,22)$ Steiner system which we denote by W_{22}. The automorphism group $Aut(W_{22})$ acts 3-transitively on the points of W_{22}.*

PROOF. Most of the work has already been done. To prove the existence of such a Steiner system we start with $PG_2(4)$, add a new point α, and new blocks $\mathcal{H}_i$ where $\mathcal{H}_i$ is a $PSL_3(4)$-orbit of hyperovals. Then Theorem 6.6B shows that we have an $S(3,6,22)$ Steiner system.

We now prove uniqueness. Consider an arbitrary $S(3,6,22)$ Steiner system W and choose one of its points α. The contraction of W at α is an $S(2,5,21)$ Steiner system, so by Theorem 6.6A we may assume that this contraction is $PG_2(4)$. Then the blocks Δ not containing α form a set $\mathcal{H}$ of 56 hyperovals in $PG_2(4)$ which cover each triangle exactly once. To show that W is isomorphic to W_{22} we shall show that $\mathcal{H} = \mathcal{H}_i$ for some $i =$ 1,2 or 3.

Suppose that Δ is a hyperoval from $\mathcal{H}$. Using only the property that $\mathcal{H}$ is a set of hyperovals covering each triangle once, we shall show that for any two points $\rho, \sigma \in \Delta$, there are three hyperovals in $\mathcal{H}$ which intersect Δ in exactly these points. Indeed, the points ρ, σ lie in 16 triangles, and each of these triangles lies in a unique hyperoval of $\mathcal{H}$. Since each hyperoval of $\mathcal{H}$ containing ρ, σ is counted four times in this process, there are $16/4 = 4$ hyperovals in $\mathcal{H}$ containing ρ, σ. Each hyperoval in $\mathcal{H}$ intersects Δ in at most two points, so there are $4 - 1 = 3$ hyperovals in $\mathcal{H}$ intersecting Δ in exactly the set $\{\rho, \sigma\}$ as claimed.

Since $\mathcal{H}_j$ also covers each triangle exactly once, then the argument in the preceding paragraph shows that similarly if Δ is a hyperoval from $\mathcal{H}_j$, then there are three hyperovals of $\mathcal{H}_j$ whose intersection with Δ equals $\{\rho, \sigma\}$. If Δ lies in both $\mathcal{H}$ and $\mathcal{H}_j$, then these three hyperovals must be the same since, according to Theorem 6.6C, there are only three hyperovals in $PG_2(4)$ which intersect Δ in exactly the set $\{\rho, \sigma\}$. Now there are 15 ways to choose a pair of points from Δ, and each choice determines three hyperovals which are shared by $\mathcal{H}$ and $\mathcal{H}_j$. Thus we have shown that whenever $\mathcal{H}$ and one of the $\mathcal{H}_i$ have a hyperoval in common, then they have at least at least 45 hyperovals in common. Since $\mathcal{H}$ contains a total of 56 hyperovals, and the $\mathcal{H}_i$ are disjoint, we conclude that $\mathcal{H}$ must equal one of the $\mathcal{H}_i$ as claimed. Finally, $\mathrm{Aut}(PG_2(4))$ acts transitively on $\{\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3\}$ (Theorem 6.5B) so all three possibilities generate isomorphic extensions. Thus W is isomorphic to W_{22}.

Transitivity of $\mathrm{Aut}(W_{22})$ now follows as before, from the uniqueness of the construction. The stabilizer of a point $(\mathrm{Aut}(W_{22}))_\alpha$ must fix one of the $PSL_3(4)$-orbits $\mathcal{H}_j$ and so equals $PSL_3(4)$ (Theorem 6.5B). Since $PSL_3(4)$ is 2-transitive on $PG_2(4)$, therefore $\mathrm{Aut}(W_{22})$ is 3-transitive on the points of W_{22}. This completes the proof. □

The Mathieu group M_{22} is a subgroup of $\mathrm{Aut}(W_{22})$ with index 2. It is simplest to construct M_{22} from the largest Mathieu group M_{24}, as we shall

do in the next section, but already we can see its action here. The group $(\mathrm{Aut}(W_{22}))_\alpha$ is $P\Sigma L_3(4)$ while $(M_{22})_\alpha = PSL_3(4)$.

Exercises

6.6.2 Calculate the intersection triangle for W_{22} (Exercise 6.2.5). Show that two blocks of W_{22} intersect in 0 or 2 points.

6.6.3 Prove that $\mathrm{Aut}(W_{22})$ is transitive on the 77 blocks of W_{22} and has rank 3.

6.7 The Mathieu Groups M_{23} and M_{24}

The Steiner system W_{22} can be extended twice more, each time in a unique way. In Section 6.5 we showed that $PSL_3(4)$ acting on $PG_2(4)$ has three orbits $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ of hyperovals and three orbits $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ of Fano subplanes. Label these orbits so that the hyperovals in $\mathcal{H}_i$ are the hyperovals generated by the quadrangles in the Fano subplanes in $\mathcal{F}_i$. Adding two new points α, β to $PG_2(4)$, define four types of blocks of W_{23} as follows:

(i) $\Lambda \cup \{\alpha, \beta\}$ for each line Λ of $PG_2(4)$;
(ii) $\Delta \cup \{\alpha\}$ for each hyperoval $\Delta \in \mathcal{H}_1$;
(iii) $\Delta \cup \{\beta\}$ for each hyperoval $\Delta \in \mathcal{H}_2$;
(iv) Φ for each Fano plane $\Phi \in \mathcal{F}_3$.

Theorem 6.7A. *With these blocks W_{23} is an $S(4,7,23)$ Steiner system.*

Proof. We must check that any set of four points lies in exactly one of the blocks defined above. There are 253 blocks of size 7 and 23 points. Since $253\binom{7}{4} = \binom{23}{4}$, it is enough to show that each set of four points is covered at least once. Let Π be a set of four points. If either α or β lies in Π, then we can apply arguments similar to those used in Theorem 6.6D to show that there is a block of type (i), (ii) or (iii) containing Π. On the other hand, suppose that Π contains only points from $PG_2(4)$. If these points are collinear then they lie in a block of type (i). If Π is a quadrangle then it lies in a unique hyperoval Δ. So if Π is not in a block of type (ii) or type (iii) then Δ is in $\mathcal{H}_3$ and Π is in a unique Fano subplane $\Phi \in \mathcal{F}_3$ and so is a block of type (iv). Finally, suppose that Π consists of three collinear points α, β, γ and a point δ not on this line. The triangle $\{\alpha, \beta, \delta\}$ is in a unique hyperoval of $\mathcal{H}_3$ (Theorem 6.6B). The line through γ and δ meets the hyperoval again at some point ζ (Exercise 6.5.10). The quadrangle $\{\alpha, \beta, \delta, \zeta\}$ is contained in a unique Fano subplane Φ which by the construction must lie in $\mathcal{F}_3$. Since γ is a diagonal point of this quadrangle, Π is contained in Φ and hence lies in a block of type (iv). This completes the proof. □

Now suppose that W is any $S(4,7,23)$ Steiner system. Its contraction at a point α is a copy of the unique $S(3,6,22)$-design constructed in Section 6.6.

Thus taking two points α, β of W, the blocks containing at least one of these points are essentially as described in (i),(ii) and (iii) of the construction of W_{22}. There remain 120 further blocks to be identified which cover exactly once each of the sets of four points not already covered by a block of type (i),(ii) or (iii). We shall repeatedly use the fact that when W is contracted twice, at any two points, the result is the projective plane $PG_2(4)$.

Theorem 6.7B. *Up to isomorphism there is a unique $S(4,7,23)$ Steiner system W_{23}. Its automorphism group $M_{23} := \mathrm{Aut}(W_{23})$ is 4-transitive on the points of W_{23}.*

PROOF. We have seen in Theorem 6.7A that an $S(4,7,23)$ Steiner system W_{23} exists, so it remains to show that every $S(4,7,23)$ Steiner system W is isomorphic to W_{23}.

By the preceding discussion we may assume that W is an extension of $PG_2(4)$ by two new points α, β. The blocks of W then consist of: (i) $\Lambda \cup \{\alpha, \beta\}$ for each line Λ of $PG_2(4)$; (ii) $\Delta \cup \{\alpha\}$ for each hyperoval $\Delta \in \mathcal{H}_1$; (iii) $\Delta \cup \{\beta\}$ for each hyperoval $\Delta \in \mathcal{H}_2$; and (iv) 120 further blocks each of which consists of seven points from $PG_2(4)$ such that each of these blocks has at most three points in common with each of the blocks of types (i)–(iii) and with each of the other blocks of type (iv). We shall denote the set of blocks of type (iv) by $\mathcal{F}$. It remains to show that $\mathcal{F} = \mathcal{F}_3$ (see the definition of W_{23}).

First, we show that each block Φ in $\mathcal{F}$ is a Fano subplane of $PG_2(4)$. To see this, take two points ρ, σ of Φ and let Λ be the line of $PG_2(4)$ through ρ and σ. As noted above, Φ and Λ cannot have more than 3 points in common. The contraction $W_{\rho,\sigma}$ is a replica of $PG_2(4)$ and the two sets $\Phi \setminus \{\rho, \sigma\}$ and $\Lambda \cup \{\alpha, \beta\} \setminus \{\rho, \sigma\}$ are lines in this projective plane. Hence these sets have a point τ in common, and so Φ and Λ have the three points ρ, σ, τ in common. Thus Φ is a set of seven points in $PG_2(4)$ with the property that any line meeting the set in more than one point meets it in three points. Therefore Φ is a Fano subplane by Exercise 6.5.6.

To complete the proof, we must show that the set $\mathcal{F}$ of Fano subplanes is actually the set $\mathcal{F}_3$. Take $\Phi \in \mathcal{F}$ and let Ξ be a quadrangle in Φ. Then Ξ is in a unique hyperoval Δ, and Δ cannot be in $\mathcal{H}_1$ or $\mathcal{H}_2$ since Φ has at most three points in common with the hyperovals in these sets. Thus $\Delta \in \mathcal{H}_3$ and $\Phi \in \mathcal{F}_3$. Since $\mathcal{F}$ and $\mathcal{F}_3$ each contain 120 Fano subplanes we conclude that $\mathcal{F} = \mathcal{F}_3$.

Thus the design W_{23} is unique up to isomorphism. As before we can use the uniqueness of W_{23}, and the fact that $\mathrm{Aut}(PG_2(4))$ acts transitively on the two sets $\{\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3\}$ and $\{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3\}$ to show that $M_{23} := \mathrm{Aut}(W_{23})$ is transitive on the points of W_{23}. The stabilizer $\mathrm{Aut}(W_{23})_{\alpha,\beta}$ fixes each of the sets $\mathcal{H}_1, \mathcal{H}_2$ and $\mathcal{F}_3$, and so it contains $PSL_3(4)$ since these sets are $PSL_3(4)$-orbits. Finally since $PSL_3(4)$ is 2-transitive, M_{23} is 4-transitive. □

Exercises

6.7.1 The two point stabilizer $(M_{23})_{\alpha\beta}$ is $PSL_3(4)$. The order of M_{23} is $23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 4$.

6.7.2 The setwise stabilizer $(M_{23})_{\{\alpha,\beta\}}$ acts on the projective plane $PG_2(4)$. Describe this action.

The last and largest of the Mathieu groups is M_{24} which acts as the group of automorphisms of the unique $S(5,8,24)$ Steiner system W_{24}. In many ways this is a remarkable group and it contains the other Mathieu groups as subgroups in natural ways. We shall construct W_{24} as an extension of W_{23} so we shall think of W_{24} as $PG_2(4)$ with three new points α, β, γ added. This Steiner system has 759 blocks where those which include any of the new points are built from lines, hyperovals and Fano subplanes of $PG_2(4)$. There is a set $\mathcal{M}$ of 210 further blocks, each of which is a set of eight points of $PG_2(4)$ and which contains at most four points in common with any line, hyperoval or Fano subplane of $PG_2(4)$. We shall show that the blocks $\Sigma \in \mathcal{M}$ are precisely those sets of points which lie on a pair of lines of $PG_2(4)$ when we omit the point of intersection. With this in mind we establish the following result.

Lemma 6.7A. *Suppose that Σ is a set of eight points of $PG_2(4)$ such that any line of $PG_2(4)$ which meets Σ in at least three points actually meets Σ in four points. Then there exist two lines Λ_1 and Λ_2 of $PG_2(4)$ such that $\Sigma = (\Lambda_1 \cup \Lambda_2) \setminus (\Lambda_1 \cap \Lambda_2)$.*

PROOF. A subset of $PG_2(4)$ with no collinear triples has at most six points. Thus Σ contains three points on some line Λ_1, and hence four points on Λ_1, by the hypothesis on Σ.

Let Λ_2 be the line joining two points of $\Sigma \setminus \Lambda_1$. We claim that the point σ of intersection of Λ_1 and Λ_2 lies outside of Σ. Suppose the contrary. Then Λ_2 would also contain four points of Σ. This would leave one point μ of Σ not on Λ_1 or Λ_2. There are three lines of $PG_2(4)$ joining μ to points of $\Lambda_2 \setminus \{\sigma\}$. At least two of these lines intersect Λ_1 in a point of Σ. Thus these lines contain three points of Σ and so, by hypothesis, contain four points of Σ. This would imply that Σ has more than eight points contrary to hypothesis. Thus we have shown that every line Λ_2 which joins two points of $\Sigma \setminus \Lambda_1$ intersects Λ_1 in the point τ of Λ_1 which is not in Σ; hence the four points of $\Sigma \setminus \Lambda_1$ are collinear. This proves the lemma. □

Theorem 6.7C. *Up to isomorphism, there is a unique $S(5,8,24)$ Steiner system W_{24}. Its automorphism group $M_{24} := \mathrm{Aut}(W_{24})$ is 5-transitive on the points of W_{24}.*

PROOF. We construct W_{24} from $PG_2(4)$ by adding three new points α, β, γ. Let $\mathcal{M}$ denote the set of all eight-point subsets of $PG_2(4)$ consisting of the points on a pair of lines of $PG_2(4)$ excluding the point of

intersection. Thus $|\mathcal{M}| = \binom{21}{2} = 210$. Also the $PSL_3(4)$-orbits of hyperplanes and Fano subplanes, namely $\mathcal{H}_i$ and $\mathcal{F}_i$ $(i = 1, 2, 3)$, are defined as before.

We define the blocks of W_{24} as follows:

(i) $\Lambda \cup \{\alpha, \beta, \gamma\}$ for each line Λ of $PG_2(4)$;
(ii) $\Delta \cup \{\alpha, \beta\}$ for each hyperoval $\Delta \in \mathcal{H}_1$;
(iii) $\Delta \cup \{\alpha, \gamma\}$ for each hyperoval $\Delta \in \mathcal{H}_2$;
(iv) $\Delta \cup \{\beta, \gamma\}$ for each hyperoval $\Delta \in \mathcal{H}_3$;
(v) $\Phi \cup \{\alpha\}$ for each Fano plane $\Phi \in \mathcal{F}_1$;
(vi) $\Phi \cup \{\beta\}$ for each Fano plane $\Phi \in \mathcal{F}_2$;
(vii) $\Phi \cup \{\gamma\}$ for each Fano plane $\Phi \in \mathcal{F}_3$;
(viii) Σ where $\Sigma \in \mathcal{M}$.

This defines a total of 759 blocks and in order to prove that this set of blocks defines W_{24} as an $S(5, 8, 24)$ Steiner system we must show that each subset of five points from W_{24} lies in exactly one of these blocks. Since $\binom{24}{5} = 759\binom{8}{5}$, it is enough to show that each set of five points lies in at least one block. The proof that we have defined a Steiner system as claimed is now similar to the earlier proofs and is left as an exercise (Exercise 6.7.3).

Finally, let $M_{24} := \mathrm{Aut}(W_{24})$. As in previous arguments we see that M_{24} is transitive. Moreover, since $\mathcal{M}$ is invariant under $\mathrm{Aut}(PG_2(4))$, it is certainly invariant under $PSL_3(4)$. Thus $(M_{24})_\alpha$ is the full automorphism group of W_{23}. Since M_{23} is 4-transitive, M_{24} must be 5-transitive. □

The setwise stabilizer $(M_{24})_{\{\alpha,\beta\}}$ is the full automorphism group of W_{22}. The Mathieu group M_{22} is the subgroup $(M_{24})_{\alpha\beta}$ of index 2.

Some of the information about the Mathieu groups and their Steiner systems is summarized in Tables 6.1 and 6.2.

Exercises

6.7.3 Show that each set of five points of W_{24} is contained in at least one of the blocks defined in (i)–(viii) in the proof of Theorem 6.7C.

TABLE 6.1. The Mathieu Groups

group	degree	transitivity	rank on blocks	order
M_{10}	10	3		$2^4 \cdot 3^2 \cdot 5$
M_{11}	11	4	4, primitive	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
M_{12}	12	5	3, on pairs	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
M_{22}	22	3	3, primitive	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
M_{23}	23	4	3, primitive	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	24	5	4, primitive	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$

TABLE 6.2. The Steiner Systems of the Mathieu Groups

Steiner system	parameters	number of blocks	automorphism group
W_{10}	(3,4,10)	30	$M_{10} \cdot 2$
W_{11}	(4,5,11)	66	M_{11}
W_{12}	(5,6,12)	132	M_{12}
W_{22}	(3,6,22)	77	$M_{22} \cdot 2$
W_{23}	(4,7,23)	253	M_{23}
W_{24}	(5,8,24)	759	M_{24}

6.7.4 Show that the set stabilizer $(M_{24})_{\{\Delta\}}$ of a block Δ of the Steiner system W_{24} induces $Alt(\Delta)$ on Δ. Describe the action of this stabilizer on the complementary set of 16 points.

6.7.5 Show that any two distinct blocks of W_{24} intersect in either 0, 2 or 4 points.

6.8 The Geometry of W_{24}

The Steiner system W_{24} has a rich geometry. Inside this geometry we are able to identify not only the Steiner systems W_{22} and W_{23} but also the Steiner systems W_{11} and W_{12}. By locating the Steiner system W_{12}, it is possible to identify a 3-transitive action of M_{11} of degree 12. Moving in the other direction to larger combinatorial structures, the geometry of W_{24} has been used to construct the Golay binary codes and also the Leech lattice in $\mathbb{R}^{24}$.

We shall begin our detailed study of the geometry of W_{24} with a lemma concerning the blocks. Recall that the symmetric difference of two sets Σ and Λ is

$$\Sigma \ominus \Lambda := \{\alpha \mid \alpha \in \Sigma \cup \Lambda, \alpha \notin \Sigma \cap \Lambda\}.$$

Lemma 6.8A. *Consider the Steiner system W_{24}.*
(i) *Two blocks intersect in 0, 2 or 4 points.*
(ii) *If two blocks intersect in four points then their symmetric difference is a block.*

PROOF. (i) This is Exercise 6.7.5. It follows either from the concrete construction of W_{24} in the last section or by calculating the intersection triangle from the parameters (Exercise 6.2.5).

(ii) Suppose that Σ_1 and Σ_2 are blocks with $\Sigma_1 \cap \Sigma_2 = \{\alpha, \beta, \gamma, \delta\}$. Contraction of W_{24} at α, β, γ gives a copy of $PG_2(4)$ with the blocks Σ_1, Σ_2

represented as lines Λ_1, Λ_2 through δ. Then according to our construction of W_{24}, the set $(\Lambda_1 \cup \Lambda_2) \setminus \{\delta\}$ is a block and it is also the symmetric difference $\Sigma_1 \ominus \Sigma_2$. □

Two distinct blocks cannot contain more than four points in common. Thus the blocks which contain a given set of four points partition the remaining 20 points of W_{24} into five sets of size four. In particular any set of four points is in exactly five blocks.

Lemma 6.8B. *Let Σ be a set of four points and Π be a block disjoint from Σ. Then in the set $\mathcal{F}$ of five blocks containing Σ either:*
(i) *two of these blocks meet Π in four points and three are disjoint from Π; or*
(ii) *four of the blocks meet Π in two points and one is disjoint from Π.*

PROOF. As we noted above, every two blocks in $\mathcal{F}$ intersect exactly in Σ. Suppose some block $\Delta_1 \in \mathcal{F}$ meets Π in four points. Then, by Theorem 6.8A, $\Delta_2 := \Delta_1 \ominus \Pi \in \mathcal{F}$ and Δ_2 also meets Π in four points. If another block from $\mathcal{F}$ intersected Π nontrivially, it would share at least one point with Δ_1 or Δ_2 which is impossible. Thus the other three blocks in $\mathcal{F}$ are disjoint from Π. This is case (i).

Now suppose that no block in $\mathcal{F}$ meets Π in four points. Then by Lemma 6.8A all the blocks in $\mathcal{F}$ intersect Π in 0 or 2 points. Since for each $\alpha \in \Pi$ there is a unique block containing $\Sigma \cup \{\alpha\}$, there are exactly four blocks in $\mathcal{F}$ which intersect Π in two points. This is case (ii). □

If two blocks Δ_1, Δ_2 of W_{24} meet in two points then their symmetric difference $\Delta_1 \ominus \Delta_2$ is a set of 12 points which we call a *dodecad*. A remarkable fact is that the stabilizer of a dodecad Γ in M_{24} induces the Mathieu group M_{12} on Γ. This means that all five of the Mathieu groups live inside M_{24}. The following result takes us part of the way toward establishing this claim.

Lemma 6.8C. *Let Γ be a dodecad of W_{24} and suppose that Δ is a block which meets Γ in at least five points. Then:*
(i) *the block Δ meets the dodecad Γ in exactly six points; and*
(ii) *there is a unique block Δ^* such that $\Gamma = \Delta \ominus \Delta^*$.*

PROOF. Since blocks intersect in an even number of points, a block must intersect a symmetric difference of blocks in an even number of points. Thus, if a block Δ meets Γ in at least five points, it must meet Γ in six or eight points. So to establish part (i) it is enough to show that a dodecad cannot contain a block.

We can write the dodecad Γ in the form $\Pi_1 \ominus \Pi_2$ with blocks Π_1 and Π_2; note that $\Pi_1 \cap \Pi_2$ contains two points. Suppose that Γ contained a block Δ. Then Δ would intersect each of Π_1 and Π_2 in four points. Since

$\Sigma := \Delta \cap \Pi_1$ and Π_2 are disjoint, and Π_1 is a block containing Σ and intersecting Π_2 in two points, Lemma 6.7B shows that no block which contains Σ can intersect Π_2 in four points. Since $|\Delta \cap \Pi_2| = 4$ we reach a contradiction. Thus every block which meets Γ in at least five points must intersect Γ in exactly six points. This proves (i).

Now suppose that Δ meets Γ in exactly six points. Then with perhaps a change in the roles of Π_1 and Π_2 we can assume that Δ meets Π_1 in four points, and so $\Delta \ominus \Pi_1$ is also a block by Lemma 6.8A. This block meets Π_2 in four points; namely, the two points of $\Delta \cap \Pi_2$ and the two points of $\Pi_1 \cap \Pi_2$. Thus Lemma 6.8A shows that $\Delta^* := (\Delta \ominus \Pi_1) \ominus \Pi_2$ is a block and $\Delta^* \ominus \Delta = \Gamma$ (see Exercise 6.8.1). □

Exercises

6.8.1 Show that the symmetric difference operation $\ominus$ is commutative and associative, and for any sets Δ, Γ we have $((\Gamma \ominus \Delta) \ominus \Delta) = \Gamma$.

6.8.2 Consider the set E of matrices of the form:

$$\begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & 0 & 1 \end{bmatrix} \quad \text{where } \alpha, \beta \in \mathbb{F}_4.$$

Show that E is an elementary abelian subgroup of $SL_3(4)$ which fixes each point on the line [1,0,0] and acts regularly on the set of points of $PG_2(4)$ which are not on this line. Deduce that the pointwise stabilizer $(M_{24})_\Delta$ of a block Δ of W_{24} acts regularly on the complement of the block.

6.8.3 Show that the pointwise stabilizer $(M_{24})_\Gamma$ of a dodecad Γ is trivial.

6.8.4 Show that W_{24} has $16 \cdot 7 \cdot 23 = 2576$ dodecads.

6.8.5 Is the complement of a dodecad in W_{24} also a dodecad?

Since every set of five points of a dodecad Γ is contained in a unique block of W_{24}, we can define a Steiner system whose point set is Γ and whose blocks are the 6-element subsets of Γ obtained by intersecting Γ with blocks of W_{24} (Lemma 6.8C). According to Theorem 2.3B this $S(5,6,12)$ Steiner system must be isomorphic to W_{12}.

Theorem 6.8A. *M_{24} acts transitively on the set of all dodecads of W_{24}, and for any dodecad Γ the setwise stabilizer $(M_{24})_{\{\Gamma\}}$ is isomorphic to M_{12}.*

PROOF. We have just noted that the stabilizer $(M_{24})_{\{\Gamma\}}$ is an automorphism group of an $S(5,6,12)$ Steiner system with Γ as point set. Since $(M_{24})_{\{\Gamma\}}$ acts faithful on Γ (Exercise 6.8.3), $(M_{24})_{\{\Gamma\}}$ is isomorphic to a subgroup H of M_{12}. The index $|M_{24} : (M_{24})_{\{\Gamma\}}|$ equals the number of dodecads lying in the orbit of Γ under M_{24}, and so is at most 2576 by Exercise 6.8.4. However, $|M_{24}| / |M_{12}| = 2576$, and so we conclude that $|M_{24} : (M_{24})_{\{\Gamma\}}| = 2576$. Hence there is a single orbit of dodecads under M_{24}, and $(M_{24})_{\{\Gamma\}} \cong H = M_{12}$ as required. □

In Section 6.5, we constructed the group M_{12} as the last in a series of transitive extensions and now we have just used the uniqueness of the $S(5,6,12)$ Steiner system W_{12} to identify the group M_{12} as a subgroup of M_{24}. An alternative approach to the Mathieu groups is possible by defining M_{12} to be the setwise stabilizer of a dodecad Γ in M_{24}, and then showing that M_{12} is 5-transitive on Γ. See the following exercise.

Exercises

6.8.6 Let Γ be a dodecad of W_{24}, and let $(\alpha_1, \ldots, \alpha_5)$ and $(\beta_1, \ldots, \beta_5)$ be any two sequences of five distinct points from Γ. Show that there is an element $z \in H := (M_{24})_{\{\Gamma\}}$ such that $(\alpha_1, \ldots, \alpha_5)^z = (\beta_1, \ldots, \beta_5)$. [*Hint:* Since M_{24} is 5-transitive there exists $x \in M_{24}$ such that $(\alpha_1, \ldots, \alpha_5)^x = (\beta_1, \ldots, \beta_5)$, so it is enough to show that there exists $y \in M_{24}$ such that y fixes $(\beta_1, \ldots, \beta_5)$ and $xy \in H$. First show that there exist blocks Σ_i $(i = 1,2,3)$ of W_{24} such that $\{\alpha_1, \ldots, \alpha_5\} \subseteq \Sigma_1, \Gamma = \Sigma_1 \ominus \Sigma_2$ and $\Gamma = \Sigma_1 \ominus \Sigma_3$, and that the blocks Σ_3 and Σ_2 each meet Σ_1 in two points outside of $\{\beta_1, \ldots, \beta_5\}$. Finally apply Exercise 6.7.4.]

6.8.7 Let Γ be a dodecad and write $\Gamma = \Delta \ominus \Delta^*$ where Δ and Δ^* are blocks of W_{24}, and put $H := (M_{24})_{\{\Gamma\}}$. Show that $H_{\{\Delta\}}$ induces the full symmetric group on each of the 6-point sets $\Delta \cap \Gamma$ and $\Delta^* \cap \Gamma$, but that these actions are not equivalent.

There is one further exceptional multiply transitive permutation action hidden inside M_{24}. If Γ is a dodecad then the complement of Γ is again a dodecad Γ^*. If we take $\alpha \in \Gamma$, then the stabilizer $(M_{12})_\alpha$ is the Mathieu group M_{11} in its natural (4-transitive) action on $\Gamma \setminus \{\alpha\}$. This group M_{11} also acts on the 12 points of Γ^*. The remarkable fact is that M_{11} is 3-transitive in this action. The geometry preserved by this 3-transitive action is not a Steiner system but a block design with blocks of size 6 in which any 3 points are together in exactly 2 blocks. This degree 12 action of M_{11} is constructed, by a different method, in Example 7.5.2.

Exercises

6.8.8 The following are some of the maximal subgroups of M_{24} described in its action on W_{24}. (The group M_{24} has nine conjugacy classes of maximal subgroups in all.)
- (i) The stabilizer of 1 point (M_{23}).
- (ii) The setwise stabilizer of 2 points ($M_{22} : 2$).
- (iii) The setwise stabilizer of 3 points ($PSL_3(4) : \Sigma_3$).
- (iv) The stabilizer of a block ($2^4 \cdot A_8$).
- (v) The stabilizer of a complementary pair of dodecads ($M_{12} : 2$).

6.8.9 Show that the stabilizer, in M_{24}, of a block induces A_8 on the block and the kernel of this action induces an elementary abelian regular group on the 16 points of the complement. Hence prove that $A_8 \cong PSL_4(2)$.

6.8.10 Mathieu's definitions: [taken from Carmichael (1937)]:
(i) $M_{11} = \langle s, t\rangle$ and $M_{12} = \langle s, t, u\rangle$ where

$$s = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10),$$
$$t = (4\ 5\ 3\ 9)(10\ 7\ 2\ 6),$$
$$u = (0\ 11)(1\ 10)(2\ 5)(3\ 7)(4\ 8)(6\ 9).$$

(ii) $M_{23} = \langle a, b\rangle$ and $M_{24} = \langle a, b, c\rangle$ where

$$a = (0\ 1\ 2\ 3\ 4\ 5\ \ldots\ 21\ 22),$$
$$b = (2\ 16\ 9\ 6\ 8)(4\ 3\ 12\ 13\ 18)(10\ 11\ 22\ 7\ 17)(20\ 15\ 14\ 19\ 21),$$
$$c = (0\ 23)(1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(18\ 14).$$

6.9 Notes

The Mathieu groups appeared first in Mathieu (1861) and Mathieu (1873) as part of a systematic study of multiply transitive groups. They were recognized as simple groups three decades later: M_{11} by Cole (1894), M_{12}, M_{22}, M_{23} and M_{24} by Miller (1899) and (1900). Steiner systems have a history going back to the early nineteenth century. The development of the Steiner systems for the Mathieu groups is presented in Carmichael (1937), Witt (1938a) and (1938b). Our presentation here owes a debt to Lüneburg (1969). There are many constructions known for these groups. A few are mentioned below; there are more in Conway and Sloane (1988) and the references given in Conway et al. (1985).

- The Witt geometries W_{12} and W_{24} can be constructed using the natural actions of the groups $PSL_2(11)$ and $PSL_2(23)$; the other geometries and groups are then defined from these. See Beth et al. (1993).
- Transitive extensions as presented in Sect. 7.4 can be used. See Rotman (1995) (who then derives the Witt geometries from the groups) and Passman (1968).
- The Golay code is the unique twelve dimensional subspace of $\mathbb{F}_2^{24}$ in which the minimum number of nonzero coordinates in a nonzero vector is 8. The Mathieu group M_{24} is the group of coordinate permutations that leave this subspace invariant. See Cameron and van Lint (1991), Conway (1971).
- R.T. Curtis has developed a remarkable method for computing the blocks of W_{24}. His Miracle Octad Generator is described in Curtis (1976) and Conway (1984).
- Exercise 6.1.2: See Chapman (1995).

7

Multiply Transitive Groups

7.1 Introduction

A permutation group G acting on a set Ω is k-transitive if any k-tuple of distinct points can be mapped, by some element of G, to any other k-tuple of distinct points. Clearly a k-transitive group is also $(k-1)$-transitive. A group is called *multiply transitive* if it is at least 2-transitive. We have already seen some examples of multiply transitive groups such as the alternating and symmetric groups, the affine groups $AGL_d(F)$ and projective groups $PGL_d(F)$ (see Sect. 2.8), and the Mathieu groups (Chap. 6).

A 2-transitive group is necessarily primitive. In our analysis of finite primitive groups in Chap. 4 we showed that the socle of a finite 2-transitive group is either elementary abelian and regular, or primitive and simple (Theorem 4.1B). Historically, this result has implications working in two directions. On the one hand, much energy has been expended in this century looking for new finite 2-transitive groups, since any new 2-transitive non-affine group would have a new simple group as its socle. On the other hand, the classification of finite simple groups leads to a classification of the finite 2-transitive groups via a determination of the primitive actions of the simple groups. The complete list of finite 2-transitive groups (8 infinite families and 10 isolated groups) is presented in Sect. 7.7.

The landscape of the infinite case is quite different. On the one hand there are infinite analogues of some of the finite groups. For example, there are various symmetric groups (see Chap. 8), and affine and projective groups can be defined over infinite fields or with infinite dimensions. These examples retain much of the structure of their finite counterparts, but infinite multiply transitive groups can also exhibit behaviour that is just not possible for a finite group, such as the nontrivial highly transitive groups. New methods, including ideas from model theory in logic, have been employed recently in an attempt to understand these infinite groups.

By definition, G acts k-transitively on Ω if and only if it acts transitively on $\Omega^{(k)}$; so in this case the stabilizers G_{α_1} of k distinct points are conjugate in G. We say that G is *sharply k-transitive* if each of these k-point

stabilizers equals 1, or equivalently, if G acts regularly on $\Omega^{(k)}$. In particular, 1-transitive and sharply 1-transitive are equivalent to transitive and regular, respectively. If $k > 1$, then clearly G is k-transitive if and only if G is $(k-1)$-transitive and each of the (conjugate) $(k-1)$-point stabilizers is transitive on the set of remaining points; we say that G is *k-primitive* if this action of the $(k-1)$-point stabilizers is primitive.

Exercises

7.1.1 Let Homeo($\mathbb{R}$) denote the set of "homeomorphisms" of $\mathbb{R}$, that is, the set of all bijections x of $\mathbb{R}$ onto itself for which x and x^{-1} are both continuous (such a mapping is called *bicontinuous*). Show that Homeo($\mathbb{R}$) is a subgroup of $Sym(\mathbb{R})$, and that a permutation x lies in Homeo($\mathbb{R}$) if and only if x is monotonic (order preserving or order reversing). [*Hint:* Use the intermediate value theorem.]

7.1.2 Let G be the set of all monotonic permutations in $Sym(\mathbb{Q})$. Show that G is 2-transitive but not 3-transitive. (See also Exercise 2.2.8.)

The following exercise deals with the group Homeo($\mathbb{Q}$) of homeomorphisms of $\mathbb{Q}$ consisting of all bicontinuous mappings of $\mathbb{Q}$ onto itself. Because $\mathbb{Q}$ is disconnected, Homeo($\mathbb{Q}$) has a much richer structure than Homeo($\mathbb{R}$).

Exercises

7.1.3 Show that every monotonic permutation of $\mathbb{Q}$ lies in Homeo($\mathbb{Q}$).

7.1.4 Suppose that I and J are any two nonempty intervals of $\mathbb{Q}$ whose end points are either irrational or infinite. Show that there is a bicontinuous mapping of I onto J.

7.1.5 Suppose that $\mathbb{Q}$ is partitioned into a finite set of intervals $I_1, \dots, I_n$ whose end points are irrational or infinite. Suppose $i \mapsto i'$ is a permutation of $\{1, 2, \dots, n\}$, and that for each i there is a bicontinuous mapping $x_i : I_i \to I_{i'}$. Let x be the permutation of $\mathbb{Q}$ whose restriction to I_i is equal to x_i $(i = 1, \dots, n)$. Show that $x \in$ Homeo($\mathbb{Q}$).

7.1.6 Show that Homeo($\mathbb{Q}$) is highly transitive.

In this chapter we shall develop some basic results on multiply transitive groups, and look at some special classes of these groups. The following elementary result will be frequently used.

Lemma 7.1A (Jordan–Witt Lemma). *Let $G \leq Sym(\Omega)$ be k-transitive for some $k \geq 1$, and let Δ be a subset of Ω with $|\Delta| = k$. Put $H := G_{(\Delta)}$ and suppose that $K \leq H$ has the property:*

$$\text{(7.1)} \qquad \begin{array}{c} \textit{for each } x \in G \textit{ such that } x^{-1}Kx \leq H \\ \textit{there exists } y \in H \textit{ such that } x^{-1}Kx = y^{-1}Ky. \end{array}$$

Let $\Gamma := \mathrm{fix}(K) \supseteq \Delta$, *and put* $N := N_G(K)$. *Then* Γ *is* N*-invariant, and* N *acts* k*-transitively on* Γ.

Remark. Two natural cases where condition (7.1) holds are when $K = H$ and (for H finite) when K is a Sylow subgroup of H.

PROOF. For each $\gamma \in \Gamma$ and $x \in N$, $(\gamma^x)^K = \gamma^{Kx} = \{\gamma^x\}$, and so $\gamma^x \in \Gamma$. This proves that Γ is N-invariant.

Now, since G is k-transitive, in order to prove that N acts k-transitively on Γ it is enough to show that:

$$\text{for each } x \in G \text{ such that } \Delta^x \subseteq \Gamma \\ \text{there exists } z \in N \text{ such that } xz^{-1} \text{ acts trivially on } \Delta. \tag{7.2}$$

However, $\Delta^x \subseteq \Gamma$ implies that xKx^{-1} acts trivially on Δ, and so $xKx^{-1} \leq H$. Thus by condition (7.1) there exists $y \in H$ such that $xKx^{-1} = y^{-1}Ky$, and so $z := yx$ satisfies the condition (7.2). □

Exercises

The following series of exercises leads to a generalization of the Jordan–Witt Lemma. Suppose that G is a group acting on a set Ω, $\alpha \in \Omega$, and $H \leq G$ with $\alpha \in \Delta := \mathrm{fix}(H)$. Put $K := N_G(H)$ and

$$\Sigma := \{x^{-1}Hx \mid x \in G \text{ and } x^{-1}Hx \leq G_\alpha\}.$$

We consider the actions of K on Δ and of G_α (by conjugation) on Σ.

7.1.7 Put $W := \{x \in G \mid \alpha^x \in \Delta\}$. Show that W is the union of a set Λ of complete double cosets of the form $G_\alpha yK$, and that $\Sigma = \{xHx^{-1} \mid x \in W\}$.

7.1.8 Show that there is a bijection Φ of Λ onto the set $\mathrm{Orb}(K, \Delta)$ of orbits of K on Δ given by $\Phi(D) := \alpha^D$.

7.1.9 Show that there is a bijection Ψ of Λ onto the set $\mathrm{Orb}(G_\alpha, \Sigma)$ of orbits of G_α on Σ given by

$$\Psi(D) := \{xHx^{-1} \mid x \in D\}.$$

7.1.10 Show that the number of (right) G_α-cosets in D is equal to $|\Phi(D)|$, and the number of (left) K-cosets in D is equal to $|\Psi(D)|$ for each $D \in \Lambda$.

7.1.11 Hence prove: there is a bijection Θ of $\mathrm{Orb}(G_\alpha, \Sigma)$ onto $\mathrm{Orb}(K, \Delta)$ such that when G is finite we have $|N_G(L) : N_{G_\alpha}(L)| = |\Theta(L^{G_\alpha})|$ for each $L \in \Sigma$.

7.2 Normal Subgroups

We begin our study of normal subgroups of multiply transitive groups with the case of a regular normal subgroup. We have met this situation before; Theorem 4.3B and Sect. 4.6 describe the regular normal subgroups of finite primitive groups. In the present case finiteness is not needed for the initial part of this analysis. Suppose that G is a transitive group acting on the set Ω and that H is a regular normal subgroup of G. Then the action of the stabilizer G_α on Ω is equivalent to its action on H by conjugation (see Exercise 1.6.16), and so, if G is multiply transitive, the non-identity elements of H form a single conjugacy class under the action of G_α. This places a severe restriction on H. The case where G is 2-primitive is studied in the following theorem. Exercises 7.2.3 and 7.2.4 below address the case of a 2-transitive but not a 2-primitive group.

Theorem 7.2A. *Suppose that $G \leq Sym(\Omega)$ is 2-primitive with $|\Omega| \geq 4$. If G has a regular normal subgroup H, then H is an elementary abelian 2-group of order $|\Omega|$. Moreover, if $|\Omega| \geq 5$, then G is not 3-primitive.*

PROOF. Fix $\alpha \in \Omega$. Then $K := G_\alpha$ is primitive on $\Omega \setminus \{\alpha\}$ by definition of 2-primitivity. As noted above, the action of K on Ω is equivalent to the action by conjugation of K on H, and so in the latter action K is primitive on the set $H^\#$ of nontrivial elements of H. For each $x \in H^\#$, the set $B := \{x, x^{-1}\}$ is a block for K, and so primitivity shows that $B = H^\#$ or $|B| = 1$. Since $|H| > 3$, this shows that each element in $H^\#$ has order 2. Thus H is an elementary abelian 2-group (see Exercise 7.2.1 below). Finally, suppose $|\Omega| > 4$ and consider the action of K on the set of ordered pairs $(H^\#)^{(2)}$. The group H has a proper subgroup A of order 4. Let B be the set of all pairs (x, y) such that $A = \langle x, y\rangle$. Then $|B| = 6$ and B is a proper block for the action of K on $(H^\#)^{(2)}$ and so K is not 2-primitive on $H^\#$. Thus G is not 3-primitive on Ω. □

In the last theorem we can identify the normal elementary abelian subgroup with the additive group of a vector space over the field $\mathbb{F}_2$. So the group G is acting as an affine group containing the translations and the stabilizer G_0 is a (possibly infinite dimensional) linear group over $\mathbb{F}_2$.

Exercises

7.2.1 Show that a group in which each nontrivial element has order 2 is an elementary abelian 2-group. [*Hint:* If $x^2 = y^2 = 1$ then $x^{-1}y^{-1}xy = (xy)^2$.]

7.2.2 Find all 2-primitive subgroups of S_n for $n \leq 4$.

7.2.3 Show that, if G is a finite 2-transitive group with a regular normal subgroup H, then H is an elementary abelian p-group for some prime p.

7.2.4 The result of the previous exercise is no longer true if G is not assumed to be finite. For example, let S be an infinite group in which all nontrivial elements are conjugate [see Higman et al. (1949)]. Take G as the image in $Sym(S)$ of $S \times S$ acting on S by

$$a^{(s,t)} := s^{-1}at \quad \text{for } a \in S \text{ and } (s,t) \in S \times S.$$

Show that G is 2-transitive and has two regular normal subgroups isomorphic to the simple group S. (This type of action is also considered in Exercises 1.4.5, 4.4.7 and 4.4.8.)

We know that a nontrivial normal subgroup of a primitive group is transitive (Theorem 1.6A). The following is an analogous result for k-primitive groups.

Theorem 7.2B. *Let $G \leq Sym(\Omega)$ be a k-primitive group for some integer $k \geq 2$ and $|\Omega| \geq 6$, and let H be a nontrivial normal subgroup of G. Then either*

(i) *H is k-transitive; or*

(ii) *$k = 2$ and H is a regular elementary abelian 2-group.*

Proof. Since G is primitive, H is certainly transitive. Fix $\alpha \in \Omega$. Then $K := G_\alpha$ is $(k-1)$-primitive on $\Omega' := \Omega \setminus \{\alpha\}$, and $M := H_\alpha \lhd K$.

If $k = 2$, then K is primitive on Ω', and so either M is trivial or M is transitive on Ω'. In the former case, H is regular, and hence, by the previous theorem, the subgroup H is an elementary abelian 2-group. In the latter case, H is 2-transitive. This proves the assertion for $k = 2$.

Now suppose $k \geq 3$ and proceed by induction. Theorem 7.2A shows that H is not regular and so $M \neq 1$. Thus, since K is $(k-1)$-primitive on Ω', induction shows that M is either regular or $(k-1)$-transitive on Ω'. In the latter case H is k-transitive and we are finished, so it remains to prove that M is not regular. Suppose that M is regular, so H is sharply 2-transitive. Choose $\beta \in \Omega'$ and put $L := G_{\alpha\beta}$ and $\Omega'' := \Omega \setminus \{\alpha, \beta\}$. Then L is $(k-2)$-primitive on Ω''. Because H is sharply 2-transitive, there exists a unique $z \in H$ such that $(\alpha,\beta)^z = (\beta,\alpha)$, and since z^2 fixes (α,β) therefore $z^2 = 1$. For each $x \in L$, the commutator $z^{-1}x^{-1}zx$ lies in H and fixes (α,β), so it is also 1. Hence z centralizes L and so the orbits of $\langle z \rangle$ on Ω'' form a system of blocks for L acting on Ω''. However the orbits of $\langle z \rangle$ all have lengths 1 or 2 and at most one has length 1 (because H is sharply 2-transitive). Since $|\Omega| > 4$, this contradicts the primitivity of L on Ω''. Hence M is not regular and the induction step is proved. □

Corollary 7.2A. *A nontrivial normal subgroup of a highly transitive group is highly transitive.*

In general a nontrivial normal subgroup of a transitive group need not be transitive, but Exercise 1.4.6 shows that at least it is true that the orbits

of the normal subgroup all have the same length. This leads to the concept of half-transitivity which we shall use below in our analysis of nonregular normal subgroups of 2-transitive groups.

We say that a nontrivial group G acting on a set Ω acts $1/2$-*transitively* if all its orbits on Ω have the same length. For each integer $k \geq 1$, we say that G acts $(k+1/2)$-*transitively* on Ω if G is k-transitive and each of the (conjugate) k-point stabilizers $G_{\alpha_1\dots\alpha_k}$ is 1/2-transitive.

Obviously

$$(k+1/2)\text{-transitivity} \Rightarrow k\text{-transitivity} \Rightarrow (k-1/2)\text{-transitivity}$$

for each integer $k \geq 1$. In general, however, it is not true that a group containing a $(k+1/2)$-transitive group is necessarily also $(k+1/2)$-transitive (see Exercise 7.2.7 below).

Exercises

7.2.5 Let $G \leq Sym(\Omega)$ be 2-transitive, and suppose that H is a nontrivial normal subgroup of G. Show that H is either regular or 3/2-transitive.

7.2.6 Let $G \leq Sym(\Omega)$ be 3-transitive, and suppose that H is a nontrivial normal subgroup of G. Show that H is either regular, 5/2-transitive or strictly 2-transitive.

7.2.7 Give an example of a permutation group G which is not 3/2-transitive but which has a normal 3/2-transitive subgroup. [*Hint:* G may be taken as a semidirect product of a regular normal elementary abelian subgroup of order 9 and a group of order 4.]

7.2.8 If G is a 1/2-transitive group of degree n, show that $|G|$ divides n.

If H is a nonregular normal subgroup of a 2-transitive group G, then a point stabilizer H_α is nontrivial and normal in G_α and so H is 3/2-transitive by Exercise 1.4.6. Is H primitive? To answer this question we shall use the concept of a minimal block: Δ is a *minimal block* for G, if Δ is a block for G containing at least two points, and no other block with at least two points is properly contained in Δ. Every finite transitive group of degree at least 2 posesses minimal blocks, but an infinite imprimitive group may not.

Exercise

7.2.9 Give an example of an infinite imprimitive group with no minimal blocks.

Theorem 7.2C. *Suppose that G is a 2-transitive subgroup of $Sym(\Omega)$ with a nontrivial imprimitive normal subgroup H. If H has a minimal block then $H_{\alpha\beta} = 1$ for every pair of distinct points $\alpha, \beta \in \Omega$. (Thus H is either regular or a Frobenius group.)*

PROOF. Let Δ be a minimal block for H. Since $H \lhd G$, Δ^x is a minimal block for H for each $x \in G$, let $\mathcal{B}$ be the set of all such blocks. Since G is

2-transitive, every pair of distinct points α, β lies in at least one block in $\mathcal{B}$. On the other hand if Δ_1, Δ_2 were distinct blocks in $\mathcal{B}$ containing α and β, then $\Delta_1 \cap \Delta_2$ would be a nontrivial block for H properly contained in Δ_1 and this contradicts the minimality of Δ_1. Hence for each pair α, β of distinct points contained in Ω, there is exactly one block in $\mathcal{B}$ containing both these points. (This shows that $\mathcal{B}$ is set of blocks for a Steiner system on Ω as discussed in Sect. 6.2).

Each block Γ containing α is fixed setwise by H_α. Thus $H_{\alpha\beta}$ fixes all blocks in $\mathcal{B}$ which contain α or β. Let Δ_0 be the block in $\mathcal{B}$ which contains α and β, and suppose that $\gamma \in \Omega \setminus \Delta_0$. Then there exist distinct blocks $\Delta_1, \Delta_2 \in \mathcal{B}$ such that $\{\alpha, \gamma\} \subseteq \Delta_1$ and $\{\beta, \gamma\} \subseteq \Delta_2$, and so $\Delta_1 \cap \Delta_2 = \{\gamma\}$. Thus $H_{\alpha\beta}$ fixes every point not lying in Δ_0. Finally, since $\Delta \neq \Omega$, there is a block $\Delta_3 \in \mathcal{B}$ with $\Delta_0 \cap \Delta_3 = \emptyset$. Since $H_{\alpha\beta}$ fixes all points in Δ_3, the argument above shows that it also fixes all points outside of Δ_3, and so $H_{\alpha\beta} = 1$ as asserted. □

Exercise

7.2.10 Let $G = AGL_d(F) \leq Sym(F^d)$ for some field F and some integer $d \geq 1$. Let H be the normal subgroup consisting of the elements of the form $v \mapsto \lambda v + a$ where $\lambda \neq 0$ is an element of F and $a \in F^d$. Show that the blocks in $\mathcal{B}$ which occur in the proof above are exactly the lines in the affine space.

Theorem 7.2D. *Let $G \leq Sym(\Omega)$ be an infinite 2-transitive group, and suppose that $H \leq G$ has finite index. Then H is primitive.*

PROOF. Every subgroup of finite index in G contains a subgroup of finite index which is normal in G (see Exercise 1.3.4), and so it is enough to prove the result under the assumption that H is normal. Thus suppose that $H \lhd G$. Since G is 2-transitive, and $H \neq 1$, therefore H is transitive and $G = G_\alpha H$. Thus $|G_\alpha : H_\alpha| = |G_\alpha H : H| = |G : H|$, and so H_α is a normal subgroup of finite index in G_α. Since G_α is transitive on $\Omega \setminus \{\alpha\}$, H_α has only a finite number of orbits on $\Omega \setminus \{\alpha\}$, all of which are infinite (Theorem 1.6A).

Now suppose that H is imprimitive. If Δ is a block for H containing α, then Δ is H_α-invariant. Since H_α has only a finite number of orbits, this shows that there are only finitely many blocks for H containing α. In particular, H has a minimal block Δ containing α. Let $\mathcal{B} := \{\Delta^x \mid x \in G\}$. Then it follows from the proof of Theorem 7.2C that any two blocks in $\mathcal{B}$ meet in at most one point and any two points are in a unique block. Choose a block $\Gamma \in \mathcal{B}$ that is disjoint from Δ, say some other block from the same system. Then each $\gamma \in \Gamma$ determines a distinct block $\Lambda_{\alpha,\gamma}$ meeting Δ in $\{\alpha\}$ and Γ in $\{\gamma\}$. Since Γ is infinite, this implies that H has infinitely many distinct blocks containing α, contrary to what we showed above. Thus H is primitive as claimed. □

For finite groups we have a stronger result (Theorem 4.1B) which we proved using the O'Nan–Scott Theorem in Chap. 4. We give here a brief alternative proof based on the structure of finite Frobenius groups. Note that the two conclusions of the theorem are not exclusive since both include the case where $\mathrm{soc}(G)$ is cyclic of prime order.

Theorem 7.2E (= Theorem 4.1B). *Let $G \leq Sym(\Omega)$ be a finite 2-transitive group. Then* $\mathrm{soc}(G)$ *is either*

(i) *primitive and simple; or*

(ii) *regular and elementary abelian.*

PROOF. Put $H := \mathrm{soc}(G)$. If H is not primitive, then Theorem 7.2.A shows that either H is regular, or H is a Frobenius group (Sect. 3.4). In the former case H is elementary abelian (see Exercise 7.2.3) and so (ii) holds. The latter case cannot hold since the structure theorem for finite frobenius groups (Sect. 3.4) shows that a finite Frobenius group has a proper nontrivial characteristic subgroup which is impossible for the socle of a finite primitive group (see Corollary 4.3B). This settles the imprimitive case.

Now suppose that H is primitive but not regular. Then H is 3/2-transitive because $H \lhd G$ (Exercise 7.2.5). By Theorem 4.3B, a finite primitive group either has a unique minimal normal subgroup, or it has exactly two minimal normal subgroups which are nonabelian, regular and isomorphic to one another. Since H is its own socle, it is a direct product of simple groups. Thus either H is simple or $H = S \times T$ where S and T are isomorphic simple, nonabelian, regular subgroups. However, in the latter case $|H| = |\Omega|^2$ which is not possible since the 3/2-transitivity of H implies that $|H|$ has a factor in common with $|\Omega| - 1$. Thus H is simple and the proof of the theorem is complete. □

The final theorem of this section strengthens Theorem 7.2E (Theorem 4.1B) in a special case.

Theorem 7.2F. *Suppose that G is a 2-transitive subgroup of $Sym(\Omega)$ of degree $2m$ where $m > 1$ is odd. Then* $\mathrm{soc}(G)$ *is a simple 2-transitive subgroup.*

PROOF. Indeed, since $2m$ is not a prime power, the previous theorem shows that $H := \mathrm{soc}(G)$ is primitive, simple and nonabelian. It follows from Exercise 1.6.12 that $|H|$ is divisible by 4. Let α and β be distinct points in Ω. To prove that H is 2-transitive it is enough to show that $G_\alpha = H_\alpha G_{\alpha\beta}$, since then H_α acts transitively on $\Omega' := \Omega \setminus \{\alpha\}$. Since $H_\alpha \lhd G_\alpha$, the group H_α acts 1/2-transitively on Ω', and so $|H_\alpha : H_{\alpha\beta}|$ divides $2m - 1$. Thus, $H_{\alpha\beta}$ contains a Sylow 2-subgroup, say P, of H_α, and $P \neq 1$ because $|H|$ is a multiple of 4. The Frattini argument (Exercise 1.4.14) shows that $G_\alpha = H_\alpha(N \cap G_\alpha)$ where $N := N_G(P)$. Since $|H : H_\alpha| = 2m$, any Sylow 2-subgroup Q of H containing P satisfies $|Q : P| = 2$, and therefore $Q \leq N$.

On the other hand the Jordan–Witt Lemma (Lemma 7.1A) shows that N leaves $\Gamma := \mathrm{fix}(P)$ invariant and acts 2-transitively on this set. Since $|Q| \nmid |G_\alpha|$ we have $Q^\Gamma \neq 1$. Thus Q^Γ has order 2, and is a Sylow 2-subgroup of the 2-transitive group N^Γ. Hence its degree $|\Gamma| = 2m - |\mathrm{supp}(P)|$ has the form $2n$ where n is odd. Applying Exercise 1.6.12 to N^Γ shows that this is impossible unless $|\Gamma| = 2$. Hence $\Gamma = \mathrm{fix}(P) = \{\alpha, \beta\}$, and so $N \cap G_\alpha \leq G_{\alpha\beta}$. This shows that $G_\alpha = H_\alpha(N \cap G_\alpha) = H_\alpha G_{\alpha\beta}$ as required. □

7.3 Limits to Multiple Transitivity

It is a consequence of the classification of finite simple groups that a finite permutation group which does not contain the alternating group is at most 5-transitive. Except for the alternating and symmetric groups, the only finite groups which are 4- or 5-transitive are the Mathieu groups M_{11}, M_{12}, M_{23} and M_{24}. The proof of this strong statement involves a case-by-case analysis of the finite simple groups. We shall be content here with a weaker result due to Wielandt (1960a) which shows that the Schreier Conjecture implies that every proper finite multiply transitive group is at most 7-transitive. (Note that the proof of the Schreier Conjecture also uses the "classification".) H. Nagao and M. Suzuki have shown how to reduce the bound in the theorem from 7 to 6 by a similar argument. The story is quite different for infinite permutation groups. For example, Homeo($\mathbb{Q}$) is highly transitive (Exercise 7.1.6), and we shall see later that, for each k, there are infinite groups that are k- but not $(k+1)$-transitive.

Recall that the Schreier conjecture states that the outer automorphism group of any finite simple group is solvable (see Appendix A).

Theorem 7.3A (Assuming the Schreier Conjecture). *Let $G \leq Sym(\Omega)$ be an 8-transitive group of finite degree. Then $G \geq Alt(\Omega)$.*

PROOF. Clearly we can assume that $|\Omega| > 8$. Fix $\Delta \subseteq \Omega$ with $|\Delta| = 5$, and put $\Gamma := \Omega \setminus \Delta$. Define $N := N_G(G_{(\Delta)})$ and $H := \mathrm{soc}(G_{(\Delta)})$ where $H \lhd N$ because the socle of a group is a characteristic subgroup. Since $\Delta = \mathrm{fix}(G_{(\Delta)})$, the Jordan–Witt Lemma (Lemma 7.1A) shows that N acts 5-transitively on Δ; hence $N^\Delta = Sym(\Delta)$. Because $G_{(\Delta)}$ acts 2-transitively on its support Γ, Theorem 4.1B shows that H is either a simple group (possibly of prime order) acting primitively on Γ, or H is an elementary abelian p-group of order $\geq p^2$ (for some prime p) acting regularly on Γ. We consider these two possibilities.

Suppose that H is simple, and put $C := C_N(H)$. The action of N on H by conjugation defines a homomorphism $\psi : N \to \mathrm{Aut}(H)$ whose kernel is C. Moreover, we have $\psi(H) = \mathrm{Inn}(H)$, and so $N/CH \cong \psi(N)/\psi(H)$ is solvable by the Schreier Conjecture. Since $N^\Delta = Sym(\Delta)$, we conclude

that

$$Alt(\Delta) \leq (CH)^{\Delta} = C^{\Delta} \leq Sym(\Delta)$$

because $Alt(\Delta)$ is simple and nonabelian. On the other hand, since H acts primitively on its support Γ, Theorem 4.3B shows that $C^{\Gamma} = H^{\Gamma}$ or 1 depending on whether H^{Γ} is regular (of prime order p, say) or not. Since $|\Gamma| > 2$, we conclude that in either case C^{Γ} and C^{Δ} have no common nontrivial homomorphic image. Hence $C = C^{\Gamma} \times C^{\Delta}$ by Theorem 1.6C, which shows that C (and hence G) contains a 3-cycle from $Alt(\Delta)$. Since G is primitive, Theorem 3.3A now shows that $G \geq Alt(\Omega)$, and the theorem is proved in this case. Note that up to this point of the proof we have only used the hypothesis that G is 7-transitive, and that $|\Omega| > 7$.

Now suppose that H is regular on Γ. Since G is 8-transitive, N^{Γ} is 3-transitive, and so by Theorem 7.2A, $H \cong H^{\Gamma}$ is an elementary abelian 2-group and hence $|\Gamma| = 2^s$ for some integer $s > 1$. Now choose $\gamma \in \Gamma$, and put $G^* := G_{\gamma}$. Since G^* is 7-transitive on $\Omega' := \Omega \setminus \{\gamma\}$, the argument above (with G^* in place of G) shows that either $G^* \geq Alt(\Omega')$ (and hence $G \geq Alt(\Omega)$), or $H^* := \mathrm{soc}(G^*)$ is an elementary abelian p-group of order $\geq p^2$ which acts regularly on $\Gamma \setminus \{\gamma\}$. However the latter cannot hold since it implies that $2^s - 1 = |\Gamma| - 1 = p^r$ for some integer $r > 1$ which is impossible by Exercise 7.3.1 below. Hence we have proved that $G \geq Alt(\Omega)$ in this case as well. □

Exercises

7.3.1 Show that if p is a prime and $p^r = 2^s \pm 1$, for positive integers r and s, then either $r = 1$ or $p = 3$, $r = 2$. [*Hint:* First show that if r is odd then the second factor in $(p^r \pm 1) = (p \pm 1)(p^{r-1} \mp \ldots + 1)$ must be odd. Also $(p^{2t} - 1) = (p^t - 1)(p^t + 1)$ and $p^{2t} + 1 \equiv 2 \bmod 4$ for p odd.] (More generally, it is true that the only solution to $p^r = q^s - 1$ with p, q primes and r, s integers > 1 is $2^3 = 3^2 - 1$.)

7.3.2 Show that the only finite solvable permutation group which is 3-primitive is the symmetric group of degree 4.

7.4 Jordan Groups

Let G be a group acting on a set Ω. We say $\Gamma \subseteq \Omega$ is a *Jordan set* and its complement $\Delta := \Omega \setminus \Gamma$ a *Jordan complement* if $|\Gamma| > 1$ and $G_{(\Delta)}$ acts transitively on Γ (the case $\Delta = \emptyset$ is permitted). If G is k-transitive on Ω, every subset Δ of size $< k$ is a Jordan complement; in such a case we say Γ and Δ are *improper*, and otherwise they are *proper*. A group G acting on Ω is a *Jordan group* if it is transitive and has at least one proper Jordan complement. These groups fit naturally into the study of multiply

transitive groups since a primitive Jordan group with a finite proper Jordan complement is always 2-transitive (see Theorem 7.4A).

Exercises

7.4.1 Let $G := AGL_d(F)$ be the affine group acting on the d-dimensional vector space $\Omega := F^d$ over the field F. If $d \geq 2$, show that every affine subspace of dimension $< d$ in Ω is a Jordan complement.

7.4.2 Let $G := PGL_{d+1}(F)$ be the projective linear group acting on the set $\Omega := PG_d(F)$. If $d \geq 3$, show that any proper projective subspace of Ω is a Jordan complement.

7.4.3 Let $G := \mathrm{Aut}(\mathbb{Q}, \leq)$ be the group of order preserving permutations of the rational numbers. Show that G is primitive, but not 2-transitive, and that every open interval Γ is a Jordan set on which $G_{(\Omega \setminus \Gamma)}$ acts primitively.

The finite Jordan groups have been completely classified using the classification of finite simple groups; except for a small handful of exceptional groups, the finite Jordan groups are closely related to the groups described in Exercises 7.4.1 and 7.4.2 above (with F finite). However the theory of finite Jordan groups which we develop here is quite elementary. Essentially it is due to Jordan and others in the last century. We shall present these results for Jordan groups under the hypothesis that the Jordan complement is finite. Jordan groups with infinite Jordan complements, such as the example in Exercise 7.4.3 above, must be handled by a different approach. There is a growing collection of recent results that deal with this case; see the notes at the end of the chapter.

The theory of Jordan groups has a geometrical flavour. We have seen in the exercises above that the Jordan complements of the affine and projective groups are the geometric subspaces. In general the finite proper Jordan complements of a primitive group behave like subspaces.

Let G be a group acting transitively on a set Ω. The properties established in the following exercises will be used repeatedly.

Exercises

7.4.4 If Δ is a Jordan complement for G then, for each $x \in G$, the set Δ^x is also a Jordan complement.

7.4.5 If Δ' and Δ are Jordan complements for G and $\Delta \cup \Delta' \neq \Omega$, then $\Delta \cap \Delta'$ is also a Jordan complement. [*Hint:* $G_{(\Delta \cap \Delta')}$ contains both $G_{(\Delta)}$ and $G_{(\Delta')}$.]

Let G be a group which acts transitively on the set Ω. A *J-flag* for G is a finite chain of distinct finite Jordan complements Δ_i for G of the form

$$\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$$

with the property that whenever Δ is a Jordan complement for G with $\Delta_{i-1} \subseteq \Delta \subseteq \Delta_i$ then $\Delta = \Delta_{i-1}$ or Δ_i. Note that $|\Omega \setminus \Delta_k| > 1$ by the

definition of Jordan complement. In the extreme case that $|\Delta_i \setminus \Delta_{i-1}| = 1$ for all $i \le j$, then G is $(j+1)$-transitive. We also note that for each $i \le k, \emptyset = \Delta_i \setminus \Delta_i \subset \ldots \subset \Delta_k \setminus \Delta_i$ is a J-flag for $G_{(\Delta_i)}$ acting on $\Omega \setminus \Delta_i$. Clearly, if $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$ is a J-flag, then $\emptyset = \Delta_0^x \subset \Delta_1^x \subset \ldots \subset \Delta_k^x$ is also a J-flag for each $x \in G$; thus G acts on the set of J-flags. Our first results show how a Jordan group acts on the set of its J-flags.

Lemma 7.4A. *Suppose that the group G acts transitively on Ω.*

(i) *If Δ and Δ' are finite Jordan complements for G with $|\Delta| \le |\Delta'|$, then $\Delta^x \subseteq \Delta'$ for some $x \in G$.*

(ii) *If $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$ and $\emptyset = \Delta_0' \subset \Delta_1' \subset \ldots \subset \Delta_\ell'$ are two J-flags for G with $|\Delta_k| = |\Delta_\ell'|$, then $k = \ell$ and for some $x \in G$ we have $\Delta_i' = \Delta_i^x$ for each i.*

PROOF. (i) By hypothesis $\Delta' \ne \Omega$, so take $\alpha \notin \Delta'$. Since G is transitive and $\Delta \ne \Omega$, there exists $y \in G$ such that $\alpha \notin \Delta^y$, and so $\Delta^y \cup \Delta' \ne \Omega$. Hence, if we choose $x \in G$ such that $\Delta^x \cap \Delta'$ is as large as possible, then $\Delta^x \cup \Delta' \ne \Omega$, and so $\Delta^x \cap \Delta'$ is a Jordan complement by Exercise 7.4.5. We claim that $\Delta^x \subseteq \Delta'$. Indeed, otherwise there exists $\beta \in \Delta^x \setminus \Delta'$ and (since $|\Delta'| \ge |\Delta|$) also some $\gamma \in \Delta' \setminus \Delta^x$. Since $\beta, \gamma \in \Omega \setminus (\Delta^x \cap \Delta')$ and $\Delta^x \cap \Delta'$ is a Jordan complement, there exists $z \in G_{(\Delta^x \cap \Delta')}$ which maps β onto γ. But then

$$\Delta^x \cap \Delta' = (\Delta^x \cap \Delta')^z \subseteq \Delta^{xz} \cap \Delta'$$

while $\gamma = \beta^z$ lies in the second of these sets but not the first. This implies that $|\Delta^x \cap \Delta'| < |\Delta^{xz} \cap \Delta'|$, contrary to the choice of x. Thus $\Delta^x \subseteq \Delta'$ as required.

(ii) We proceed by induction on $|\Delta|$. The result is true for $\Delta = \emptyset$, so suppose $\Delta \ne \emptyset$. Then k and ℓ are both at least 1, and it follows from (i) that for some $y \in G$ either $\Delta_1^y \subseteq \Delta_1'$ or $\Delta_1^y \supseteq \Delta_1'$. By the properties of a J-flag this implies that $\Delta_1 = \Delta_1'$. Now

$$\emptyset = \Delta_1^y \setminus \Delta_1' \subset \ldots \subset \Delta_k^y \setminus \Delta_1'$$

and

$$\emptyset = \Delta_1' \setminus \Delta_1' \subset \ldots \subset \Delta_\ell' \setminus \Delta_1'$$

are J-flags for $G_{(\Delta_1')}$ acting on $\Omega \setminus \Delta_1'$. Hence induction shows that $k = \ell$ and that for some $z \in G_{(\Delta_1)}$ we have $(\Delta_i' \setminus \Delta_1') = (\Delta_i^{yz} \setminus \Delta_1')$ for each $i \ge 1$. The result now follows with $x = yz$. □

If G is an imprimitive Jordan group then the blocks of imprimitivity and the Jordan complements must fit together in a particular way. This is useful even for primitive Jordan groups since these groups are generally built up from smaller degree imprimitive Jordan groups. This is the content of the following lemma.

Lemma 7.4B. *Let G be a group acting transitively on Ω.*

(i) *Suppose that G is imprimitive and that $\mathcal{B}$ is a system of nontrivial blocks for G. If G has a Jordan complement Δ then, either there exist a block $\Gamma \in \mathcal{B}$ such that $\Delta \cup \Gamma = \Omega$, or else Δ is a union of some subset $\mathcal{B}'$ of blocks from $\mathcal{B}$ with $|\mathcal{B} \setminus \mathcal{B}'| > 1$. Moreover, in the latter case $\mathcal{B}'$ is a Jordan complement for G acting on $\mathcal{B}$.*

(ii) *If $\Delta' \subseteq \Delta$ are two Jordan complements for G with $|\Delta \setminus \Delta'| < |\Omega \setminus \Delta|$ then, for any system $\mathcal{B}$ of nontrivial blocks for $G_{(\Delta')}$ acting on $\Omega \setminus \Delta'$, the set $\Delta \setminus \Delta'$ is a union of blocks from $\mathcal{B}$.*

(iii) *If G is primitive and $\Delta' \subset \Delta$ are consecutive terms in a J-flag for G, then $\Lambda := \Delta \setminus \Delta'$ is a block for the action of $G_{\{\Delta'\}}$ acting on $\Omega \setminus \Delta'$, and $\Omega \setminus \Delta$ is a union of at least two blocks from the corresponding system of blocks.*

PROOF. (i) If Δ is not a union of blocks from $\mathcal{B}$, then there exists a block $\Gamma \in \mathcal{B}$ such that $\Delta \cap \Gamma \neq \emptyset$ or Γ. Since $G_{(\Delta)}$ is transitive on $\Omega \setminus \Delta$, this shows that $\Gamma \supseteq \Omega \setminus \Delta$ as asserted. Now suppose that $\Delta \cup \Gamma \neq \Omega$ for every $\Gamma \in \mathcal{B}$. Then Δ is a union of a subset $\mathcal{B}'$ of blocks from $\mathcal{B}$ with $|\mathcal{B} \setminus \mathcal{B}'| > 1$. In the action of G on $\mathcal{B}$ we clearly have $G_{(\mathcal{B}')} \geq G_{(\Delta)}$, and so $G_{(\mathcal{B}')}$ acts transitively on $\mathcal{B} \setminus \mathcal{B}'$; this shows that $\mathcal{B}'$ is a Jordan complement.

(ii) This follows immediately from (i) applied to $G_{(\Delta')}$ acting on $\Omega \setminus \Delta'$ since the condition on $|\Omega \setminus \Delta|$ shows that $\Omega \setminus \Delta$ is not contained in a block of $\mathcal{B}$.

(iii) Put $\Lambda := \Delta \setminus \Delta'$. We first show that $|\Lambda| < |\Omega \setminus \Delta|$. This is immediately true if Ω is infinite, and so suppose that Ω is finite. Since G is primitive, $\Omega \setminus \Delta$ is not a block for G and so there exists $x \in G$ such that $\Sigma := \Delta \cap \Delta^x \neq \Delta$ and $\Delta \cup \Delta^x \neq \Omega$. By Exercise 7.4.5, Σ is a Jordan complement for G properly contained in Δ, and so by Lemma 7.4A (ii) we conclude that $\Sigma^y \subseteq \Delta'$ for some $y \in G$. Thus $|\Sigma| \leq |\Delta'|$ and so

$$|\Lambda| = |\Delta \setminus \Delta'| \leq |\Delta \setminus \Sigma| = |(\Delta^x \cup \Delta) \setminus \Delta| < |\Omega \setminus \Delta|$$

which proves our claim.

We now show that Λ is a block for $G_{\{\Delta'\}}$ acting on $\Omega \setminus \Delta'$. Suppose the contrary. Then there exists $x \in G_{\{\Delta'\}}$ such that $\Lambda \cap \Lambda^x \neq \Lambda$ or $\emptyset$. Since $\Delta = \Delta' \cup \Lambda$ we have $\Delta' \subset \Delta \cap \Delta^x \subset \Delta$, and $|\Delta \cup \Delta^x| = |\Delta \cup \Lambda^x| < |\Omega|$ by the assertion which we just proved. Exercise 7.4.5 now shows that $\Delta \cap \Delta^x$ is a Jordan complement for G, and it lies properly between Δ' and Δ contrary to the choice of Δ'. Thus we conclude that Λ is a block for $G_{\{\Delta'\}}$; since $|\Lambda| < |\Omega \setminus \Delta|$, (ii) is proved. □

With this collection of technical details in hand we can proceed to a remarkable series of criteria for multiple transitivity for Jordan groups obtained by Jordan (1871).

Theorem 7.4A. *Let G be a group acting primitively on Ω.*

(i) *If G has a finite nonempty Jordan complement then G is 2-transitive.*

(ii) *If G has a finite Jordan complement Δ such that $G_{(\Delta)}$ has no nontrivial blocks of size less than $|\Delta|$ on $\Omega \setminus \Delta$, then G is $(|\Delta| + 1)$-transitive.*

(iii) *If G has two finite Jordan complements $\Delta' \subset \Delta$ with $|\Delta \setminus \Delta'| = 1$ then G is $(|\Delta| + 1)$-transitive.*

PROOF. (i) Let $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$ be a J-flag for G of length $k > 0$. Then applying Lemma 7.4B (ii) to the pair $\emptyset \subset \Delta_1$ shows that Δ_1 is a block for G, and hence $|\Delta_1| = 1$. This implies that G is 2-transitive.

(ii) We proceed by induction on $|\Delta|$. The result is true for $\Delta = \emptyset$ so suppose that $\Delta \neq \emptyset$. We first show that if $\Delta' \subset \Delta$ are consecutive terms in a J-flag for G, then $|\Delta \setminus \Delta'| = 1$. This is true if $\Delta' = \emptyset$ by (i), so suppose that $\Delta' \neq \emptyset$. Put $\Lambda := \Delta \setminus \Delta'$ and note that $|\Lambda| < |\Delta|$. Then Lemma 7.4B (ii) shows Λ is a block for $G_{\{\Delta'\}}$ acting on $\Omega \setminus \Delta'$ and that $\Omega \setminus \Delta$ is a union of a set of at least two of the blocks conjugate to Λ. Since $G_{(\Delta)} \leq G_{\{\Delta'\}}$ these latter blocks must also be blocks for $G_{(\Delta)}$ and hence must be of size 1 by the hypothesis on $G_{(\Delta)}$. Thus $|\Lambda| = 1$ as claimed. Now $|\Delta \setminus \Delta'| = 1$ and so $G_{(\Delta')}$ acts 2-transitively (and hence primitively) on $\Omega \setminus \Delta'$. Since $|\Delta| = |\Delta'| + 1$, induction now shows that G is $|\Delta|$-transitive. Finally, since $G_{(\Delta)}$ is transitive on $\Omega \setminus \Delta$, the group G is $(|\Delta| + 1)$-transitive.

(iii) By the argument in (ii), $G_{(\Delta')}$ acts 2-transitively (and hence primitively) on $\Omega \setminus \Delta'$. Thus by (ii), G is $|\Delta|$-transitive. Since $G_{(\Delta)}$ is transitive, G is $(|\Delta| + 1)$-transitive. □

Exercises

7.4.6 Suppose that G is a group acting primitively on a set Ω and Δ is a finite Jordan complement. If $G_{(\Delta)}$ is an abelian group whose nontrivial elements all have order $\geq |\Delta|$, show that G is $(|\Delta| + 1)$-transitive.

7.4.7 Let G be a primitive Jordan group on a set Ω which has a finite proper Jordan complement. Show that the minimal proper Jordan sets for G form the blocks of a Steiner system on which G acts.

Let G be a primitive Jordan group with a J-flag $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$. If G is t-transitive then the increments $\Lambda_i := \Delta_i \setminus \Delta_{i-1}$ are singletons for $i = 1, \ldots, t-1$. If G is not $(t+1)$-transitive then the remaining increments Λ_i have at least two elements and Λ_i is a block of imprimitivity for $G_{(\Delta_{i-1})}$ on $\Omega \setminus \Delta_{i-1}$. The definition of Jordan group places a condition on the pointwise stabilizer of a Jordan complement Δ_i. In fact, the setwise stabilizer $G_{\{\Delta_i\}}$ induces a transitive action on Δ_i itself and $G_{\{\Delta_i\}}$ is a Jordan group on Δ_i with J-flag $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_{i-1}$. We show this in the following lemma.

Lemma 7.4C. *Let G be a group acting primitively on Ω and let*

$$\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$$

be a J-flag for G with $k \geq 1$. Then:

(i) *For each $i < k$, $G_{\{\Delta_k\}} \cap G_{(\Delta_i)}$ acts transitively on $\Delta_k \setminus \Delta_i$.*

(ii) *If* $|\Delta_k \setminus \Delta_{k-1}| > 1$ *then* $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_{k-1}$ *is a J-flag for the group* $G_{\{\Delta_k\}}$ *acting on* Δ_k.

(iii) *Let* $|\Delta_k| \geq t$. *Then* G *is* t*-transitive on* Ω *if and only if* $G_{\{\Delta_k\}}$ *acts* t*-transitively on* Δ_k.

PROOF. (i) Put $\Delta := \Delta_k$ and $\Delta' := \Delta_i$. The idea is to apply the Jordan–Witt Lemma (Lemma 7.1A) to the transitive action of $G_{(\Delta')}$ on $\Omega \setminus \Delta'$. Since $\Delta \supset \Delta'$ we have $G_{(\Delta)} < G_{(\Delta')}$. The normalizer of $G_{(\Delta)}$ in $G_{(\Delta')}$ is $G_{\{\Delta\}} \cap G_{(\Delta')}$ and the fixed point set of $G_{\{\Delta\}} \cap G_{(\Delta')}$ in its action on $\Omega \setminus \Delta'$ is exactly $\Delta \setminus \Delta'$. Moreover, for any $x \in G$ with $\Delta' \subset \Delta^x$, the set $\Delta^x \setminus \Delta'$ is a Jordan complement for $G_{(\Delta')}$ and so, by Lemma 7.4A (i), there exists $y \in G_{(\Delta')}$ such that $\Delta^x \setminus \Delta' = (\Delta \setminus \Delta')^y$. Equivalently, for all $x \in G, x^{-1}G_{(\Delta)}x \leq G_{(\Delta')}$ implies that $x^{-1}G_{(\Delta)}x = y^{-1}G_{(\Delta)}y$ for some $y \in G_{(\Delta')}$. Now the Jordan–Witt Lemma shows that $G_{\{\Delta\}} \cap G_{(\Delta')}$ acts transitively on $\Delta \setminus \Delta'$ as asserted.

(ii) Since $|\Delta_k \setminus \Delta_i| > 1$ for all $i < k$, (i) shows that each of these Δ_i is a Jordan complement for $G_{\{\Delta_k}$ acting on Δ_k. It remains to show that if Δ is a Jordan complement for $G_{\{\Delta_k}$ and $\Delta_{i-1} \subseteq \Delta \subseteq \Delta_i$ for some $i < k$, then $\Delta = \Delta_{i-1}$ or Δ_i. Indeed, the hypotheses show that $G_{\{\Delta_k\}} \cap G_{(\Delta)}$ acts transitively on $\Delta_k \setminus \Delta$ and that $G_{(\Delta_i)}$ acts transitively on $\Omega \setminus \Delta_i$. Since these two orbits intersect nontrivially and have union $\Omega \setminus \Delta$, we conclude that $G_{(\Delta)}$(which contains both $G_{\{\Delta_k\}} \cap G_{(\Delta)}$ and $G_{\{\Delta_i\}}$) acts transitively on $\Omega \setminus \Delta$. Hence Δ is a Jordan complement for G, and so $\Delta = \Delta_{i-1}$ or Δ_i by the definition of a J-flag.

(iii) It is clear that G is t-transitive if and only if whenever $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$ is a J-flag for G with $|\Delta_k| \geq t$ we have $k \geq t$ and $|\Delta_i| = i$ for $i = 0, 1, \ldots, t-1$. Thus the assertion follows immediately from (ii) or Theorem 7.4A (iii) depending on whether or not $|\Delta_k \setminus \Delta_{k-1}| > 1$. □

We now have a detailed picture of the structure of a J-flag $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$ for a Jordan group G. If G is $t-$transitive but not $(t+1)-$transitive, then the sets in the series grow one point at a time up to Δ_{t-1}. After this point the increments $\Lambda_i := \Delta_i \setminus \Delta_{i-1}$ grow in size by at least a factor of 2 at each step. This follows by applying Lemma 7.4B (iii) to the (2-transitive) action of $G_{\{\Delta_{i+1}\}}$ on Δ_{i+1}. We see that Λ_i is a block for $G_{(\Delta_{i-1})}$ and $|\Lambda_{i+1}| = |\Delta_{i+1} \setminus \Delta_i| \geq 2\,|\Lambda_i|$. For the affine and projective groups the J-flags are formed by the geometric subspaces increasing by one dimension at each step. In the case of the 3-transitive group $AGL_d(2)$ the Jordan complement Δ_i has 2^{i-1} points so the increments increase by a factor of exactly 2 each time for $i \geq 2$.

The following theorem, proved by B. Marggraff in 1889, applies the ideas developed so far.

Theorem 7.4B. *Let* G *be a group acting primitively on a finite set* Ω *of size* n*, and suppose that* G *has a Jordan complement of size* m *where* $m \geq n/2$. *Then* G *is 3-transitive, and moreover, if* $m > n/2$ *then* $G \geq Alt(\Omega)$.

PROOF. We proceed by induction on n to show that G is 3-transitive. The result is easily verified if $n \le 4$, so suppose that $n > 4$. Let $\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k$ be a J-flag for G with $|\Delta_k| = m$. By Lemma 7.4B (i) we have

$$|\Delta_k \setminus \Delta_{k-1}| \le \frac{1}{2}\,|\Omega \setminus \Delta_k| = \frac{1}{2}\,(n-m).$$

If $|\Delta_k \setminus \Delta_{k-1}| = 1$, then G is $(m+1)$-transitive by Theorem 7.4A, so suppose that $|\Delta_k \setminus \Delta_{k-1}| > 1$. Then from the inequality above and the hypothesis on m we have

$$|\Delta_{k-1}| \ge m - \frac{1}{2}(n-m) = \frac{1}{2}m + \frac{1}{2}(2m-n) \ge \frac{1}{2}m = \frac{1}{2}\,|\Delta_k|\,.$$

Hence by Lemma 7.4C (ii) and the induction hypothesis, $G_{\{\Delta_k\}}$ acts 3-transitively on Δ_k, and so Lemma 7.4C (iii) shows that G is also 3-transitive.

Now suppose that $m > n/2$. We leave the case where $n \le 7$ as an exercise, and so we assume $m \ge 5$. An induction similar to the one above shows that we may conclude that $H := G_{\{\Delta_k\}}$ restricted to Δ_k contains $Alt(\Delta_k)$. Thus the derived group H' restricted to Δ_k is equal to the simple group $Alt(\Delta_k)$, and H' restricted to $\Omega \setminus \Delta_k$ has no homomorphic image isomorphic to $Alt(\Delta_k)$ because $m > n - m$. Hence the kernel of the action of H' on $\Omega \setminus \Delta_k$ induces $Alt(\Delta_k)$ on Δ_k by Theorem 1.4B. Thus $G \ge H' \ge Alt(\Delta_k)$ and this shows that G contains a 3-cycle. Since G is primitive, Theorem 3.3.A now shows that $G \ge Alt(\Omega)$ as asserted. □

Exercises

7.4.8 Complete the proof of the theorem above for $n \le 7$.

7.4.9 In the case that $m = n/2$ and G is a proper primitive group in Marggraff's Theorem, show that there exists d such that $n = 2^d$ and $G \le AGL_d(2)$ [*Hint:* Show that there are proper Jordan complements of size 4. Pick one point to be 0 and make Ω into a vector space by defining the sum $\alpha + \beta$ to be the fourth point in the Jordan complement of order 4 containing $0, \alpha, \beta$.]

Using the classification of finite simple groups, a precise description of the finite primitive Jordan groups has been obtained; since such a group is 2-transitive it is a matter of checking the list of finite multiply transitive groups (see Sect. 7.7). If G is a finite primitive Jordan group acting on a set Ω then one of the following cases applies.

(i) Ω is the affine space $AG_d(q)$ of dimension d over the field $\mathbb{F}_q$ and $ASL_d(q) \le G \le A\Gamma L_d(q)$ for some $d \ge 2$ and prime power q.

(ii) Ω is the projective space $PG_d(q)$ of dimension d over the field $\mathbb{F}_q$ and $PSL_{d+1}(q) \le G \le P\Gamma L_{d+1}(q)$ for some $d \ge 2$ and prime power q.

(iii) Ω is the affine space $AG_4(2)$ of dimension 4 over the field $\mathbb{F}_2$ and $G \le AGL_4(2)$ is an extension of the group of translations by A_7. The

group G is 3-transitive and has the 2-dimensional affine subspaces as Jordan complements with 4 points.

(iv) Ω is the projective space $PG_3(2)$ of dimension 3 over the field $\mathbb{F}_2$ and $G \le PGL_3(2)$ is the stabilizer of a point in the group described in (iii).

(v) G is one of the large Mathieu groups M_{22}, $\mathrm{Aut}(M_{22})$, M_{23} and M_{24} acting on the corresponding Steiner system. The proper Jordan complements are the blocks of the Steiner systems.

The final part of this section is devoted to some classical results on special types of Jordan groups. In particular we consider primitive groups of finite degree that contain a cycle of prime power length. With this in mind we next prove a more general theorem that again goes back to the work of Jordan (1871). Some of the situations where the theorem can be applied are explored in the exercises that follow it.

Theorem 7.4C. *Let G be a group acting primitively on Ω with a finite Jordan complement Δ. Suppose that $H := G_{(\Delta)}$ acts (transitively) on $\Omega \setminus \Delta$ such that for each integer d with $1 \le d < |\Delta|$ there is at most one system of imprimitivity for H whose blocks have size d. Then G is $(|\Delta|+1)$-transitive.*

PROOF. We proceed by induction on $m := |\Delta|$. We know that G is 2-transitive by Theorem 7.4A so the result is true if $m \le 1$. Suppose that $m > 1$.

First suppose that G is 3-transitive. Then for $\alpha \in \Delta$ the group G_α is 2-transitive on $\Omega \setminus \{\alpha\}$ with a Jordan complement $\Delta \setminus \{\alpha\}$ and $(G_\alpha)_{(\Delta\setminus\{\alpha\})} = H$, so induction shows that G_α is $|\Delta|$-transitive and hence G is $(|\Delta| + 1)$-transitive.

Thus we may suppose that G is not 3-transitive and $m > 1$ and produce a contradiction. In particular, $2m < |\Omega|$ by Theorem 7.4B. Moreover, if

$$\emptyset = \Delta_0 \subset \Delta_1 \subset \ldots \subset \Delta_k = \Delta$$

is a J-flag for G ending in Δ, then $|\Delta_1| = 1$ and $|\Delta_i \setminus \Delta_{i-1}| > 1$ for all $i > 1$ by Lemma 7.4B.

We claim that $k = 2$. Put $K := G_{(\Delta_{k-1})}$ and consider the action of K on $\Omega \setminus \Delta_{k-1}$; we claim that K satisfies the same hypothesis as H does. That is, if $\mathcal{B}$ and $\mathcal{B}'$ are two systems of nontrivial blocks of the same size d for the action of K on $\Omega \setminus \Delta_{k-1}$ then $\mathcal{B} = \mathcal{B}'$. Lemma 7.4B (ii) shows that $\Delta \setminus \Delta_{k-1}$ is a union of blocks (from either system) so $d \le |\Delta \setminus \Delta_{k-1}| < |\Delta|$. Also there are blocks $\Sigma \in \mathcal{B}$ and $\Sigma' \in \mathcal{B}'$ with $\Sigma, \Sigma' \subseteq \Omega \setminus \Delta$. Then Σ and Σ' are blocks for $H \le K$ acting on $\Omega \setminus \Delta$, and so the hypothesis on H shows that Σ and Σ' are conjugate under H, and hence $\mathcal{B} = \mathcal{B}'$. This shows that K satisfies the same hypothesis as H, and so we can apply induction to conclude that G is $(|\Delta_{k-1}| + 1)$-transitive. Since G is not 3-transitive, this means that $|\Delta_{k-1}| \le 1$ and so $k \le 2$. If $k \le 1$ then $m \le 1$ contrary to hypothesis, and so $k = 2$.

This shows that G has a J-flag of the form $\emptyset \subset \{\alpha\} \subset \Delta$. Now observe that, for all $x \in G$, $\Delta \cup \Delta^x \neq \Omega$ (because $2m < |\Omega|$), and so $\Sigma := \Delta \cap \Delta^x$ is a Jordan complement by Lemma 7.4A. Thus $\Sigma = \emptyset, \Delta$ or $\{\gamma\}$ for some $\gamma \in \Delta$. Moreover, if $\Sigma = \{\gamma\}$, then $\Gamma := \Delta^x \setminus \{\gamma\} \subseteq \Omega \setminus \Delta$ is a block for the action of H on $\Omega \setminus \Delta$; indeed, for each $z \in H = G_{(\Delta)}$, we have $\Delta^{xz} \cap \Delta^x \supseteq \{\gamma\}$ and so $\Gamma^z \cap \Gamma = \emptyset$ or Γ.

Finally, since G is 2-transitive, we can choose $x, y \in G$ such that

$$\Delta^x \cap \Delta = \{\alpha\}, \Delta^y \cap \Delta = \{\beta\} \text{ and } \Delta^x \cap \Delta^y = \{\gamma\}$$

for distinct points α, β and γ (choose x and y so that $\alpha^x = \alpha, \beta^x \notin \Delta$ and $\alpha^y = \gamma \in \Delta^x \setminus \Delta$). Then $\Delta^x \setminus \{\alpha\}$ and $\Delta^y \setminus \{\beta\}$ are finite blocks of size $|\Delta| - 1$ for H acting on $\Omega \setminus \Delta$, and so by the hypothesis on H they must lie in the same system of imprimitivity for H. However,

$$(\Delta^x \setminus \{\alpha\}) \cap (\Delta^y \setminus \{\beta\}) = \{\gamma\} \neq \emptyset$$

and so these two blocks must be equal. Thus

$$\Delta^x \setminus \{\alpha\} = \Delta^y \setminus \{\beta\} = \{\gamma\}$$

which shows that $|\Delta \setminus \{\alpha\}| = 1$, and then Theorem 7.4A (iii) shows that G is 3-transitive, a contradiction. This completes the proof of the theorem. □

An alternative argument, using ideas from Sect. 6.2, can be given for the end of this proof. Start at the point where we know that G has a J-flag of the form $\emptyset \subset \{\alpha\} \subset \Delta$. We claim that the images of Δ under G form the blocks for a Steiner system. Since G is 2-transitive any two points are in the same number of blocks and since the intersection of any two of these blocks is a Jordan complement for G, two points are in a unique block. The blocks meeting Δ in any fixed point form a system of imprimitivity for H on $\Omega \setminus \Delta$. So if we take points $\alpha, \beta \in \Delta$ and $\gamma \notin \Delta$ the blocks of the Steiner system through α, γ and through β, γ define two different systems of imprimitivity for H of the same size d. This is contrary to hypothesis.

Exercises

7.4.10 Show that the condition on H in Theorem 7.4C is equivalent to: if K_1 and K_2 are subgroups of the same index d in H with $1 \leq d < |\Delta|$ and these subgroups have a common fixed point on $\Omega \setminus \Delta$, then K_1 and K_2 are conjugate in H.

7.4.11 If G is a group acting primitively on a set Ω and G contains a cycle $x \neq 1$ with a finite number t of fixed points, show that G is $(t+1)$-transitive.

7.4.12 Suppose that G is a proper primitive group containing a cycle $x \neq 1$ with a finite number of fixed points. Show that $C_G(x) = \langle x \rangle$. [*Hint:* Show that otherwise there exists $w \neq 1$ in G such that $\mathrm{supp}(w) \cap$

supp(x) $= \emptyset$. Then Exercise 7.4.11 shows that $[w, z]$ is a 3-cycle for some $z \in G$.]

7.4.13 Suppose that G is a proper primitive group of degree n containing a cycle x of length $m > 1$. Show that $m \geq (n-m)! + 1$ in all cases, and that $m \geq 2(n-m)!$ when m is even. [*Hint:* Put $\Delta := \mathrm{fix}(x)$, $H := G_{\{\Delta\}}$, $K := G_{(\Delta)}$ and $C := \{y^{-1}xy \mid y \in H\}$. Show that $m\,|C| = |H| = (n-m)!\,|K|$.]

Lemma 7.4D. *Let $N \leq Sym(\Gamma)$ be a transitive group of degree p^k with a normal Sylow p-subgroup P, and suppose that P contains a cycle x of length p^k. Then the derived group $N' \leq P$.*

PROOF. We shall proceed by induction on the degree. The result is true for $k = 1$ since in this case $P = \langle x \rangle$ is a regular normal subgroup of order p and $N \leq AGL_1(p)$ (see Exercise 3.5.1). So suppose that $k > 1$. Let $Z := Z(P)$; this is a nontrivial normal subgroup of N (since the centre of a p-group is a nontrivial characteristic subgroup and $P \lhd N$). Since $\langle x \rangle$ is a regular abelian group, it is self-centralizing in $Sym(\Gamma)$ (Theorem 4.2A) and, in particular, $Z \leq \langle x \rangle$. Note that N normalizes Z and so $N/C_N(Z)$ is isomorphic to a subgroup of Aut(Z). Since Z is cyclic, Aut(Z) is abelian (see Exercise 2.2.2) and so the derived group $N' \leq C_N(Z)$. Let $\Sigma := \{\Gamma_1, \dots, \Gamma_h\}$ be the set of orbits of Z (with $h < p^k$ because $Z \neq 1$).

Now suppose that y is a p'-element of N'. We have to show that $y = 1$. Since N acts transitively on Σ and x acts as an h-cycle on Σ, we can apply induction on the degree to conclude that y acts trivially on Σ. Thus $\Gamma_i^y = \Gamma_i$ for each i. However, if γ lies in the Z-orbit Γ_i then $\gamma^y = \gamma^z$ for some $z \in Z$ which implies that $\gamma^{y^j} = \gamma^{z^j}$ for all integers j because $y \in N' \leq C_N(Z)$. Thus y acts as a p-element on Γ_i. Since y is a p'-element this implies that y acts trivially on each Γ_i. Hence $y = 1$ as required. □

The following result generalizes Theorem 3.3E.

Theorem 7.4D. *Let G be a proper primitive group of finite degree. If G contains a p^k-cycle x for some $k \geq 1$, then x has at most 2 fixed points if $p \neq 3$, and at most 3 fixed points if $p = 3$.*

PROOF. Suppose that G is acting on the set Ω of size n. Put $\Delta := \mathrm{fix}(x)$, $t := |\Delta|$ and let P be a Sylow p-subgroup of $G_{(\Delta)}$ containing x. Exercise 7.4.11 shows that G is $(t+1)$-transitive. Since $\Delta = \mathrm{fix}\,P$, the Jordan–Witt Lemma (Lemma 7.1A) shows that $N := N_G(P) \leq G_{\{\Delta\}}$ and N acts t-transitively on Δ; in other words, N^Δ is $Sym(\Delta)$. Thus $(N')^\Delta = \mathrm{Alt}(\Delta)$. On the other hand, putting $\Gamma := \Omega \setminus \Delta$, Lemma 7.4D shows that $(N')^\Gamma$ is a p-group. If $p \neq 3$ and $t \geq 3$, then we could choose $x \in N'$ such that x^Δ is a 3-cycle, and x^Γ has order p^r, say. Then x^{p^r} is a 3-cycle lying in N', which is impossible by Theorem 3.3A. Hence when $p \neq 3$, t is at most 2. Similarly, if $p = 3$ and $t \geq 4$, then we could choose $x \in N'$ such that

x^Δ is a permutation of cycle type 2^2, and again a suitable p-power of x gives a permutation of type 2^2 lying in N'. On the other hand, the degree $n = t + 3^k \geq 13$ because G cannot contain a 3-cycle, so this possibility is ruled out by Example 3.3.1. Hence, when $p = 3$, t is at most 3. This proves the theorem. □

The possible exception in the case $p = 3$ does not actually occur. Indeed the proof above shows that if the p^k-cycle has t fixed points then G is $(t+1)$-transitive. But the classification of finite simple groups shows that there are no proper 6-transitive groups and the only proper 4- and 5-transtive groups are the Mathieu groups, of degrees 11, 12, 23 and 24, none of which contains a cycle of length 3^k $(k \geq 1)$.

In fact, suppose that G is a primitive group of degree $t + p^k$ containing a p^k-cycle. If $t = 0$ then G must be 2-transitive or a subgroup of $AGL_1(p)$ (see Theorems 3.5A and 3.5B). If $t > 0$ then G is 2-transitive by Theorem 7.4A. Using the classification of 2-transitive finite groups (see Sect. 7.7) it can be shown that one of the following situations arises:

(i) $t = 0, k = 1, G \leq AGL_1(p)$;
(ii) $t = 0, G \leq P\Gamma L_d(q)$ where $p^k = \frac{q^d-1}{q-1}$ for some prime power q;
(iii) $t = 0, G = PSL_2(11)$ of degree 11, M_{11} of degree 11 or M_{23} of degree 23;
(iv) $t = 1, AGL_1(2^d) \leq G \leq AGL_d(2)$ where $2^d = 1 + p^k$ and G is 3-transitive;
(v) $t = 1, p = 2, 2^k + 1 = q$ is a Fermat prime and $G = AGL_1(q)$;
(vi) $t = 1, p = 2, k = 3$ and $G \leq AGL_2(3)$ of degree 9;
(vii) $t = 1, G = M_{11}$ of degree 12, M_{12} of degree 12 or M_{24} of degree 24;
(viii) $t = 2, p = 2, 2^k + 1 = q$ is a Fermat prime and $G = PGL_2(q)$;
(ix) $t = 2, p = 2, 2^k + 1 = 3^2,\ G = PGL_2(9)$ or $P\Gamma L_2(9)$.

Consult Exercise 7.3.1 for more insight into the prime arithmetic in parts (iv), (v), (viii) and (ix).

7.5 Transitive Extensions

If G is k-transitive on a set Ω then the stabilizer G_α is $(k-1)$-transitive on $\Omega \setminus \{\alpha\}$. The idea of a transitive extension is to reverse this process. We start with a group $H \leq Sym(\Omega)$ and pick a new point $\omega \notin \Omega$, and attempt to construct a group G acting transitively on the set $\Omega^* = \Omega \cup \{\omega\}$ such that the stabilizer G_ω is the original group H. In this case, we call G a *transitive extension* of the permutation group H. Clearly if H is k-transitive on Ω then G is $(k+1)$-transitive on Ω^*. Transitive extensions are rare in the finite case, since the new group G is multiply transitive and so is one of a slender family of groups. Working the other way around,

every multiply transive group G arises from some group H by transitive extension. Using the classification of finite 2-transitive groups in Sect. 7.7, questions about the existence or nonexistence of a transitive extension of a finite group H can be easily answered by scanning the list. On the other hand, results on transitive extensions formed an important part of the work leading up to the classification, so it seems appropriate to look at some of these more elementary results.

In this section we establish a criterion for the existence of a transitive extension of a transitive group H and apply this criterion to the construction of some exceptional 2-transitive groups. We then present a sample nonexistence theorem [due to Zassenhaus (1935)] which shows that most of the groups $PSL_d(q)$, in their natural action on the points of the projective space $PG_{d-1}(q)$, fail to have transitive extensions.

As a first step, recall the following classical result expressing the rank of a permutation group in terms of double cosets (Exercise 3.2.27). Suppose that the group G is transitive on a set Ω and that $\alpha \in \Omega$. Then G has rank r on Ω if and only if for some $y_1, \ldots, y_{r-1} \in G$ the group G is the disjoint union of r (G_α, G_α)-double cosets:

$$G = G_\alpha \cup G_\alpha y_1 G_\alpha \cdots \cup G_\alpha y_{r-1} G_\alpha.$$

If the orbits of G_α are $\Delta_0 = \{\alpha\}, \Delta_1, \ldots, \Delta_{r-1}$ then we can label the suborbits so that the double coset $G_\alpha y_i G_\alpha$ consists of the elements of G taking α to a point in Δ_i.

Suppose that H is k-transitive on Ω and set $\Omega^* = \Omega \cup \{\omega\}$ where $\omega \notin \Omega$. If $x \in Sym(\Omega^*)$ is any element that does not fix ω, then $G = \langle H, x\rangle$ will certainly be $(k+1)$-transitive, but will usually contain $Alt(\Omega^*)$. In other words, unless we choose x with care, the stabilizer G_ω will be strictly larger than H. Theorem 7.5A gives a sufficient condition for the existence of a transitive extension of a group H.

Theorem 7.5A. *Let $H \le Sym(\Omega)$ be a transitive group of rank r. Fix $\alpha \in \Omega$ and let $y_0 = 1, y_1, \ldots, y_{r-1}$ be a set of representatives for the (H_α, H_α)-double cosets in H. Now choose a point ω not in Ω and put $\Omega^* := \Omega \cup \{\omega\}$, and let $x \in Sym(\Omega^*)$ with $\omega \in$ supp(x). Then $G := \langle H, x\rangle$ is a transitive extension of H whenever the following conditions hold:*
(i) $x^2 \in H$;
(ii) $xy_ix \in HxH$ *for* $i = 1, \ldots, r-1$; *and*
(iii) $xH_\alpha x = H_\alpha$.

Remark. Exercise 7.5.1 shows that every transitive extension can be constructed in this way (with an arbitrary set of representatives for the (H_α, H_α)-double cosets) provided x is chosen appropriately.

PROOF. Put $K := H \cup HxH$. We shall first show that K is a subgroup of $Sym(\Omega^*)$. Indeed, (i) shows that K is closed under taking inverses, so

it is enough to show that $KK \subseteq K$. However, from (iii) and (ii) we have $x^{-1}H_\alpha y_i H_\alpha x^{-1} = H_\alpha x y_i x H_\alpha \subseteq HxH$ for each $i \geq 1$, and so by (i) and (iii):

$$xHx = x^{-1}Hx^{-1} = x^{-1}H_\alpha x^{-1} \cup \bigcup_{i\geq 1} x^{-1}H_\alpha y_i H_\alpha x^{-1} \subseteq H \cup HxH = K.$$

Hence $KK \subseteq H \cup HxHxH \subseteq HKH = K$ as required. Thus K is a subgroup and so $G = \langle H, x\rangle = H \cup HxH$.

Finally, $G_\omega = H$ since ω is fixed by H but not by any element in HxH. Thus G is a transitive extension of H. □

EXAMPLE 7.5.1. The symmetric group $G := S_n$ can be constructed as a transitive extension of $H := S_{n-1}$ taking $x := (n-1\ n)$, $K := S_{n-2}$ and double coset representative $y := (n-2\ n-1)$. Conditions (i)–(iii) of Theorem 7.5A are easily verified.

EXAMPLE 7.5.2. Our second example is less trivial. Let $\Delta := \{\alpha, \beta, \gamma, \delta, \epsilon\}$ and consider the action of $A := Alt(\Delta)$ on $\Omega := \Delta^{\{2\}}$. We label the ten elements of Ω as follows:

0	1	2	3	4	5	6	7	8	9
$\delta\epsilon$	$\alpha\epsilon$	$\alpha\beta$	$\beta\gamma$	$\gamma\delta$	$\alpha\gamma$	$\beta\delta$	$\gamma\epsilon$	$\delta\alpha$	$\beta\epsilon$

and calculate the images of some particular elements of A under this action:

$$\begin{array}{rcl} (\alpha\beta\gamma) & \mapsto & a = (197)(235)(486) \\ (\beta\gamma)(\epsilon\delta) & \mapsto & b = (18)(25)(49)(67) \\ (\alpha\beta)(\epsilon\delta) & \mapsto & c = (16)(35)(47)(89) \\ (\alpha\delta)(\beta\gamma) & \mapsto & y_1 = (01)(24)(56)(79) \\ (\alpha\delta)(\beta\epsilon) & \mapsto & y_2 = (02)(16)(37)(45) \end{array}$$

Then $H := \langle b, y_1\rangle \cong A$ and $H_0 = \langle a, b\rangle \cong S_3$. The orbits of H_0 are $\{0\}, \{1,4,6,7,8,9\}$ and $\{2,3,5\}$, and so $1, y_1$ and y_2 form a set of representatives for the (H_0, H_0)-double cosets in H. Let ∞ be a point not in Ω, and define $x := (\infty 0)(35)(48)(79)$. Then it is straightforward to verify that conditions (i)–(iii) of Theorem 7.5A are satisfied for $G := \langle H, x\rangle$ (observe that $(xy_1)^3 = 1$ and $(xy_2)^3 = c$). Thus G is a 2-transitive group of degree 11 and order $11 \cdot 10 \cdot 6$.

A further extension is possible in this case. Add a new point ω and define $z := (\omega\infty)(18)(47)(69)$, and note that $1, x$ are representatives of the (H, H)-double cosets in G. Again, it is easy to check that Theorem 7.5A applies to show that $F := \langle G, z\rangle$ is a transitive extension of G, and so F is a 3-transitive group of degree 12 and order $12 \cdot 11 \cdot 10 \cdot 6$.

The two groups G and F are sporadic examples of multiply transitive groups; they do not form part of an infinite family. We have met both of the groups earlier in other circumstances. The group G is isomorphic to $PSL_2(11)$, a group with a natural 2-transitive representation of degree 12.

The permutation representation of $PSL_2(11)$ of degree 11 constructed here is one of the exceptional actions of prime degree discussed at the end of Sect. 3.5. The 3-transitive group F is isomorphic to the Mathieu group M_{11}. Recall that the Mathieu group M_{24} acts on an $S(5,8,24)$ Steiner system. At the end of Chap. 6, it is mentioned that the stabilizer H in M_{24} of the symmetric difference Γ of two blocks that meet in two points is isomorphic to the group M_{12}. If $\alpha \in \Gamma$ then $H_\alpha \cong M_{11}$ and the action of this copy of M_{11} on the complement of the block Γ is the action we have just constructed under the name F.

There is something of the rabbit-out-of-the-hat about constructing a multiply transitive group by transitive extension. Once the special permutation x is defined, it is simple to check the conditions and build the group. The hard part is finding permutations that work.

Exercises

7.5.1 Suppose that $G \leq Sym(\Omega^*)$ is a 2-transitive group, $H := G_\omega$ is a point stabilizer of G, and H_α is a point stabilizer of H. Let $1, y_1, \dots, y_{r-1}$ be any set of representatives for the (H_α, H_α)-double cosets in H, and choose $x \in G$ such that x interchanges ω and α (this is possible because G is 2-transitive). Show that the conditions (i)–(iii) of Theorem 7.5A are satisfied.

7.5.2 Show that the "Klein 4-group" $H := \langle (12)(34), (13)(24) \rangle$ has no transitive extension.

7.5.3 Let $\Omega = \{0, 1, \dots, 7, 8\}$ and define the following permutations of this set:

$$a := (083)(174)(265) \qquad b := (012)(345)(678)$$
$$c := (0)(1823)(4765) \qquad d := (0)(1624)(3587).$$

(i) Show that $T := \langle a, b \rangle$ is a regular elementary abelian group of order 9 and that $H := \langle a, b, c, d \rangle$ is a sharply 2-transitive subgroup of $AGL_2(3)$ whose stabilizer $H_0 = \langle c, d \rangle$ is a quaternion group of order 8.

(ii) Add a new point ∞ to obtain $\Omega^* := \Omega \cup \{\infty\}$, and define $x = (\infty 0)(1)(2)(38)(45)(67)$. Use Theorem 7.5A to show that the group $G = H \cup HxH$ is a sharply 3-transitive group of degree 10 with stabilzer H.

(In fact, $G \cong M_{10}$ the stabilizer of a point in the Mathieu group M_{11}. We know that there are two more successive transitive extensions possible from the group $G = M_{10}$ just constructed. The next exercise explores the first of these.)

7.5.4 Let $G \cong M_{10}$ be the group constructed in Exercise 7.5.3, and let ω be a new point not in Ω^*. Define the permutation

$$z := (\omega\infty)(0)(1)(2)(36)(48)(57)$$

Use z to construct a transitive extension of G. (This extension is isomorphic to M_{11}.)

7.5.5 In Exercise 7.5.3, the regular subgroup T can be identified with the vector space $\mathbb{F}_3^2$ in such a way that the stabilizer $H_0 = \langle c, d\rangle$ acts as a linear group. Show that if a and b are taken as a basis, then the matrices representing c and d are $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, respectively. Note that $c^2 = d^2$ corresponds to a scalar matrix.

7.5.6 Let $\Gamma := \{\alpha, \beta, \gamma, \delta, \epsilon, \zeta\}$. Then $Alt(\Gamma)$ induces an action on the set of partitions of Γ into two sets of size 3. There are 10 such partitions that we label with the elements of $\Omega^* = \{0, \ldots, 8, \infty\}$ as follows:

$$\begin{array}{lll@{\qquad}lll}
\infty & : & \alpha\beta\gamma \mid \delta\epsilon\zeta & 4 & : & \alpha\gamma\epsilon \mid \beta\delta\zeta \\
0 & : & \alpha\beta\delta \mid \gamma\epsilon\zeta & 5 & : & \alpha\gamma\zeta \mid \beta\delta\epsilon \\
1 & : & \alpha\beta\epsilon \mid \gamma\delta\zeta & 6 & : & \alpha\delta\epsilon \mid \beta\gamma\zeta \\
2 & : & \alpha\beta\zeta \mid \gamma\delta\epsilon & 7 & : & \alpha\delta\zeta \mid \beta\gamma\epsilon \\
3 & : & \alpha\gamma\delta \mid \beta\epsilon\zeta & 8 & : & \alpha\epsilon\zeta \mid \beta\gamma\delta
\end{array}$$

Retaining the notation of Exercise 7.5.3, this identification defines an embedding $\Phi : Alt(\Gamma) \to Sym(\Omega^*)$. Show that under this mapping Φ we have

$$\begin{aligned}
(\alpha\beta\gamma) &\mapsto a \\
(\delta\epsilon\zeta) &\mapsto b \\
(\alpha\zeta\beta\epsilon)(\gamma\delta) &\mapsto c \\
(\alpha\beta)(\gamma\delta) &\mapsto x
\end{aligned}$$

Hence show that M_{10} has a subgroup of index 2 isomorphic to A_6. (However M_{10} is not isomorphic to S_6.)

As well as being able to construct transitive extensions, it is also valuable to know that some particular group H does not have any transitive extensions. One approach is to use Exercise 7.5.1 to prove that there are no transitive extensions by showing that there are no appropriate elements satisfying these conditions of Theorem 7.5A. Other arguments have been given over the years to show that certain groups fail to have transitive extensions. The final portion of this section applies some of these ideas to affine and projective groups.

We have seen in Chap. 6 that the group $PSL_3(4)$ has a transitive extension to the Mathieu group M_{22} and that the latter group can be extended twice more in succesion to produce M_{23} and M_{24}. On the other hand, the projective group $PSL_d(2)$ is isomorphic to the linear group $GL_d(2)$ so the affine group $AGL_d(2)$ is a transitive extension of $PSL_d(2)$. We will show that these are the only two cases in which the natural permutation action of $PSL_d(q)$ has a transitive extension. The key observations are that $PSL_d(q)$ is a Jordan group and that a transitive extension of a Jordan group is again a Jordan group.

Lemma 7.5A. *Suppose that H is a t-transitive Jordan group acting on a set Ω and that G is a transitive extension of H acting on the set $\Omega^* = \Omega \cup \{\omega\}$. Suppose that H has a proper Jordan complement Δ of size k, and that any set of t points of Ω is contained in exactly λ complements of this size. Let $v := |\Omega|$ and $\Gamma := \Delta \cup \{\omega\}$. Then*

(i) *the set Γ is a Jordan complement for G on Ω^*;*
(ii) *the group induced on Γ by $G_{\{\Gamma\}}$ is a transitive extension of the group induced on Δ by $H_{\{\Delta\}}$;*
(iii) *any $t+1$ points of Ω^* are in exactly λ Jordan complements for G of size $k+1$;*
(iv) *the number b of Jordan complements of size $k+1$ for G is*

$$b = \frac{(v+1)(v)(v-1)\cdots(v-t+1)}{(k+1)(k)(k-1)\cdots(k-t+1)}\lambda.$$

PROOF. Parts (i), (ii) and (iii) are straightforward applications of Lemmas 7.4A and 7.4C. Part (iv) follows directly from (iii). □

Suppose that the Jordan group H has a proper Jordan complement Δ and that $H^{\Delta}_{\{\Delta\}}$ does not have a transitive extension; then Lemma 7.5B shows that H does not have a transitive extension either. This idea is used in the following theorem.

Theorem 7.5B. *Let $d \geq 3$. If the group $PSL_d(q)$ in its natural action on $PG_{d-1}(q)$ has a transitive extension then either $q = 2$ or $d = 3$ and $q = 4$.*

PROOF. For the group $H := PSL_d(q)$ the Jordan complements are the proper subspaces of $PG_{d-1}(q)$. Lemma 7.5A shows that it will be enough to prove that $PSL_3(q)$ does not have a transitive extension for $q \neq 2, 4$ and that $PSL_4(4)$ does not have a transitive extension.

First consider the case where $d = 3$, and suppose that H has a transitive extension G. The geometry of the projective plane $PG_2(q)$ is an $S(2, q+1, q^2+q+1)$ Steiner system. Lemma 7.5A (iv) applies with $v = q^2+q+1$, $k = q+1$ and $\lambda = 1$, so the number b of complements of size $k+1$ for G is

$$b = \frac{(q^2+q+2)(q^2+q+1)(q^2+q)}{(q+2)(q+1)q} = \frac{(q^2+q+2)(q^2+q+1)}{(q+2)}.$$

This number must be an integer. Since $\mathrm{GCD}(q^2+q+2, q+2) = \mathrm{GCD}(q+2, 4)$ and $\mathrm{GCD}(q^2+q+1, q+2) = \mathrm{GCD}(q+2, 3)$, the group G can exist only when q is a prime power such that $q+2$ divides 12. Therefore $PSL_3(q)$ can have a transitive extension only if $q = 2$ or 4.

Now consider the group $H := PSL_4(4)$ acting on the 85 points of $\Omega := PG_3(4)$ and suppose that G is a transitive extension. The group H has Jordan complements Δ which are planes in the space Ω. In this case it is more convenient to work with these planes rather than the lines. Each

pair of points of Ω is in the same number $\lambda := q+1 = 5$ of planes and each plane has $k := q^2+q+1 = 21$ points (so the planes form a 2-$(q^3+q^2+q+1, q^2+q+1, q+1)$ design). By Lemma 7.5A (iv), the group G would have $b := \frac{86\cdot 85\cdot 84\cdot 5}{22\cdot 21\cdot 20}$ Jordan complements of size 22. Since b is not an integer, $PSL_d(4)$ does not have a transitive extension if $d \geq 4$. This completes the proof of the theorem. □

The basic idea used in the preceeding theorem is that a transitive extension of an automorphism group of a combinatorial geometry should also act on a tightly related geometry. We proved this in the case of a Jordan group and then showed that the extended geometry fails to exist. The same approach works to show that the Mathieu group M_{24} and the affine groups $AGL_d(q)$ $(d \geq 3)$ have no transitive extensions (see Exercises 7.5.8, 7.5.9). Since there do exist $S(3, q+1, q^2+1)$ and $S(3, q+1, q^2+1)$ Steiner systems (see Examples 6.2.4 and 6.2.5), the analogous method must work with the planes in the affine case and fails entirely for extensions of $AGL_2(q)$. The argument developed here can be extended to certain other groups; see Hughes (1965) and Lüneburg (1969).

Exercises

7.5.7 Complete the proof of Lemma 7.5A.

7.5.8 Show that the Mathieu group M_{24} does not have a transitive extension.

7.5.9 Show that the affine group $AGL_d(q)$ does not have a transitive extension if $d \geq 3$. [*Hint:* Apply Lemma 7.5A with Δ a plane.]

7.5.10 Show that the groups $AGL_d(2)$ are the only transitive extensions of $PGL_d(2)$. [*Hint:* Use Exercise 7.4.9.]

7.6 Sharply k-transitive Groups

In this section we consider permutation groups which are sharply k-transitive. Recall that a group $G \leq Sym(\Omega)$ is sharply k-transitive if it acts regularly on the set $\Omega^{(k)}$ of k-tuples of distinct elements of Ω. Alternatively, G is sharply k-transitive if it is k-transitive and the identity is the only element of G with more than $k-1$ fixed points. Trivially S_k is sharply k-transitive and A_k is sharply $(k-2)$-transitive, so to avoid these cases we shall require the condition that $|\Omega| > k+2$.

Sharply k-transitive groups have been studied for a long time. A classical result of Jordan (1873) runs as follows.

Theorem 7.6A. *Let G be a sharply k-transitive group of finite degree d with $d > k+2 > 5$. Then either $k = 4, d = 11$ and $G = M_{11}$, or $k = 5, d = 12$ and $G = M_{12}$.*

Much later, Tits (1952) showed that there are no infinite sharply k-transitive groups if $k \geq 4$. Both of these results are subsumed by the following theorem of Hall (1954).

Theorem 7.6B. *Let G be a 4-transitive group such that the stabilizer of 4 points is a finite group of odd order. Then G is finite and G is one of S_4, S_5, A_6, A_7 or M_{11} in its natural permutation representation.*

Finally, Yoshizawa (1979) showed, more generally, that there are no infinite 4-transitive groups in which the stabilizer of 4 points is finite.

Exercise

7.6.1 Use Theorem 7.6B to show that there are no sharply k-transitive groups when $k \geq 4$ except those listed in Theorem 7.6A.

As a consequence of these theorems, interest in sharply k-transitive groups is restricted to the cases $k = 2$ or 3. A construction of a general class of sharply 2-transitive groups and a list of seven exceptional groups were described by Dickson (1905). Zassenhaus (1936) showed that these are the only finite sharply 2-transitive groups. Zassenhaus also showed that there are exactly two infinite families of finite sharply 3-transitive groups. So far no complete description of the infinite sharply 2- and 3-transitive groups is known. In this section we describe some algebraic constructions used to study sharply 2- and 3-transitive groups.

We first consider the sharply 2-transitive groups. The 1-dimensional affine group $AGL_1(F)$ over any field F is sharply 2-transitive group in its natural action on $AG_1(F)$. Dickson generalized this example by generalizing the concept of a field.

A *near field* is a set F with at least two elements 0 and 1 and with two binary operations $+$ and $\cdot$ such that:

NF1: $(F, +)$ is an abelian group with identity 0 (we denote the inverse of α under $+$ by $-\alpha$ and use $F^{\#}$ to denote the set of nonzero elements of F);

NF2: $(F^{\#}, \cdot)$ is a group with identity 1 (we denote the inverse of α in this group by α^{-1}), and $\alpha \cdot 0 = 0 \cdot \alpha = 0$ for all $\alpha \in F$;

NF3: there is a one-sided distributive law: $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$ for all $\alpha, \beta, \gamma \in F$.

EXAMPLE 7.6.1. Every field (or even division ring) is a near field. Conversely, a near field is a field exactly in the case that the operations $+$ and $\cdot$ are both commutative.

EXAMPLE 7.6.2. An important class of near fields was described in 1905 by L. E. Dickson. These near fields are now called *Dickson near fields* (or

sometimes *regular* near fields). With seven exceptions, they include all finite near fields.

Let $(D, +, \cdot)$ be a division ring and let $\phi : D^\# \to \mathrm{Aut}(D)$ be a mapping from the group of units of D to the automorphism group of D. We require that ϕ satisfy the condition

$$\phi(\alpha^{\phi(\beta)} \cdot \beta) = \phi(\alpha)\phi(\beta) \quad \text{for all } \alpha, \beta \in D^\#. \tag{7.3}$$

We then define a new multiplication $\odot$ on $D^\#$ by

$$\alpha \odot \beta := \alpha^{\phi(\beta)} \cdot \beta \text{ for all } \alpha, \beta \in D^\#.$$

The condition (7.3) implies the identity $\phi(\alpha \odot \beta) = \phi(\alpha)\, \phi(\beta)$ and from this it is straightforward to check that $(D, +, \odot)$ is a near field.

Concrete examples of Dickson near fields can easily be given in the finite case. Let q be a prime power and n be a positive integer such that: each prime that divides n also divides $q-1$; and $n \not\equiv 0 \bmod 4$ if $q \equiv 1 \bmod 4$. These conditions ensure that n divides $(q^n - 1)/(q-1)$ and that the integers

$$1, \frac{q^2-1}{q-1}, \frac{q^3-1}{q-1}, \ldots, \frac{q^n-1}{q-1}$$

form a complete residue system modulo n (see, for example, Lüneburg (1981), Th. 6.4). Let $F := \mathbb{F}_{q^n}$ and let ω be a generator of the cyclic group $F^\#$ of units. Since n divides the order of $F^\#$, $F^\#$ has a subgroup $H := \langle \omega^n \rangle$ of index n. For $i = 1, \ldots, n$, define $\gamma_i := \omega^{(q^i-1)/(q-1)}$. Then the elements γ_i $(i = 1, \ldots, n)$ form a complete system of coset representatives for H. Consider the automorphism $\tau : \xi \mapsto \xi^q$ of F and define $\phi : F \to \mathrm{Aut}(F)$ by setting $\phi(\xi) := \tau^i$ if ξ is in the coset $H\gamma_i$. One can readily check that ϕ satisfies the condition (7.3). Let ξ, η be elements of $F^\#$ with $\phi(\xi) = \tau^i$ and $\phi(\eta) = \tau^j$. So $\xi = \alpha\gamma_i$ and $\eta = \beta\gamma_j$ for some $\alpha, \beta \in H$. Then H is a characteristic subgroup of $F^\#$, so $\xi^{\phi(\eta)}\eta = \alpha^{\tau^j}\gamma_i^{\tau^j}\beta\gamma_j \in H\gamma_i^{\tau^j}\gamma_j$. We want to show that $\gamma_i^{\tau^j}\gamma_j$ is in the coset $H\gamma_{i+j}$. But $\gamma_i^{\tau^j}\gamma_j$ is ω raised to the exponent

$$\left(\frac{q^i-1}{q-1}\right)q^j + \frac{q^j-1}{q-1} = \frac{q^{i+j}-q^j}{q-1} + \frac{q^j-1}{q-1} = \frac{q^{i+j}-1}{q-1}.$$

Thus ϕ satisfies the condition (7.3) and we have constructed a near field.

Any near field can be used to construct a sharply 2-transitive group in a way that generalizes the construction of affine groups. Let F be a near field and take $\Omega = F$. Let G^* be the set of all permutations of Ω of the form $\xi \mapsto \xi\beta + \alpha$ $(\alpha \in F, \beta \in F^\#)$, and K^* be the subset of permutations defined by mappings $\xi \mapsto \xi + \alpha$. A simple calculation shows that: G^* is a sharply 2-transitive group, K^* is a regular normal subgroup of G^*, and the point stabilizers of G^* are isomorphic to $(F^\#, \cdot)$.

This construction of sharply 2-transitive groups containing a normal abelian subgroup is quite general, as the next theorem shows.

Theorem 7.6C. *Let $|\Omega| \geq 2$ and let $G \leq Sym(\Omega)$ be a sharply 2-transitive group which possesses a regular normal abelian subgroup K. Then there exists a near field F such that G is permutation isomorphic to the group G^* defined in the construction above.*

PROOF. Take $F := \Omega$ and fix two arbitrary elements of F which we denote by 0 and 1. We shall use $a, b, c, \ldots$ to represent elements of G and $0, 1, \alpha, \beta, \ldots$ to represent elements of F. We then define binary operations $+$ and $\cdot$ on F as follows. Since K is regular, there is a bijection of K onto Ω given by $a \mapsto 0^a$. The operation $+$ on F is defined by: $0^a + 0^b = 0^c$ where $c = ab$ in K. Then $a \mapsto 0^a$ defines an isomorphism from K onto $(F, +)$. Since the point stabilizer G_0 acts regularly on $F^\# := F \setminus \{0\}$, we can similarly define $\cdot$ on $F^\#$ so that $a \mapsto 1^a$ is an isomorphism of G_0 onto $(F^\#, \cdot)$. We also define $a \cdot 0 = 0 \cdot a = 0$ for all $a \in F$. Then (NF1) and (NF2) are satisfied and it remains to show that (NF3) holds. We first establish an identity: for all $a \in K$ and $b \in G_0$ we have $b^{-1}ab \in K$ and $0^a \cdot 1^b = 0^{b^{-1}ab}$. Indeed, if $a = 1$ then $b^{-1}ab = 1$ so $0^a \cdot 1^b = 0 \cdot 1^b = 0 = 0^{b^{-1}ab}$. Suppose $a \neq 1$. Then there exists a unique $c \in G_0$ such that $0^a = 1^c$. This implies that $0^a \cdot 1^b = 1^c \cdot 1^b = 1^{cb} = 0^{ab} = 0^{b^{-1}ab}$ because $b \in G_0$. Now it is easily seen that (NF3) : $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$, holds whenever at least one variable is 0. On the other hand, suppose that $\gamma \neq 0$. Then there are $a, b \in K$ and $c \in G_0$ with $\alpha = 0^a$, $\beta = 0^b$, $\gamma = 1^c$. Now the identity just proved shows that

$$\begin{aligned}(\alpha + \beta) \cdot \gamma &= (0^a + 0^b) \cdot 1^c = 0^{ab} \cdot 1^c = 0^{c^{-1}abc} \\ &= 0^{(c^{-1}ac)(c^{-1}bc)} = 0^a \cdot 1^c + 0^b \cdot 1^c = \alpha \cdot \gamma + \beta \cdot \gamma.\end{aligned}$$

Thus F with the operations $+$ and $\cdot$ forms a near field.

Finally, we show that G is the group of all permutations of the form $\xi \mapsto \xi \cdot \beta + \alpha$. By construction, the permutations in K are defined by mappings $\xi \mapsto \xi + \alpha$ where $\alpha \in F$ and the permutations in G_0 are defined by mappings of the form $\xi \mapsto \xi \cdot \beta$ where $\beta \in F^\#$. Since K is a regular normal subgroup of G every element x of G can be written $x = ba$ where $a \in K$ and $b \in G_0$. Thus x is a permutation of the form $\xi \mapsto \xi \cdot \beta + \alpha$ with $\alpha \in F$ and $\beta \in G_0$. Since G is 2-transitive all permutations of this form are in G. □

Combining Theorem 3.4B, Example 7.6.1 and the previous theorem we get the following characterization.

Corollary 7.6A.

(i) *Every finite, sharply 2-transitive group G is permutation isomorphic to a group G^* obtained from a finite near field by the construction described above.*

(ii) *For every (possibly infinite) sharply 2-transitive group whose point stabilizers are abelian there exists a field F such that G is permutation isomorphic to the affine group $AGL_1(F) \leq Sym(F)$.*

The Dickson near fields, defined in Example 7.6.2, give examples of finite sharply 2-transitive groups contained in the group $A\Gamma L_1(q)$. Apart from these examples there are, up to permutation isomorphism, seven further finite sharply 2-transitive groups G. In each case G contains the group of translations of a vector space $\mathbb{F}_p^2$ and is contained in the group $AGL_2(p)$ where $p = 5, 7, 11, 23, 29$ or 59 (there are two examples with $p = 11$). The stabilizers G_0 for the exceptional groups are described in Table 7.1 where the given matrices generate G_0 as a subgroup of $GL_2(p)$. In the first four cases, the groups are solvable. In the remaining cases the group G_0 has the form $2 \cdot A_5 \times C$ where C is cyclic of order 1, 7 or 29, and so is not solvable.

Exercise

7.6.2 Let L be the subgroup of $SL(2, 11)$ generated by the matrices a and b listed in item V above. Show that L acts regularly on the set of nonzero vectors in the underlying vector space over $\mathbb{F}_{11}$. Hence construct a finite sharply 2-transitive permutation group of degree 121 which has a nonsolvable point stabilizer.

TABLE 7.1. Generators for the Stabilizers of the Exceptional Finite Sharply 2-transitive Groups

	p	a	b	c
(i)	5	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & -2 \\ -1 & -2 \end{bmatrix}$	
(ii)	11	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 5 \\ -5 & -2 \end{bmatrix}$	$\begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}$
(iii)	7	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 3 \\ -1 & -2 \end{bmatrix}$	
(iv)	23	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & -6 \\ 12 & -2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$
(v)	11	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 4 \\ 1 & -3 \end{bmatrix}$	
(vi)	29	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & -7 \\ -12 & -2 \end{bmatrix}$	$\begin{bmatrix} 16 & 0 \\ 0 & 16 \end{bmatrix}$
(vii)	59	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 9 & 15 \\ -10 & -10 \end{bmatrix}$	$\begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}$

Theorem 7.6C and its corollary raises the natural question: when does an infinite sharply 2-transitive group $G \leq Sym(\Omega)$ have a regular normal abelian subgroup? Since a sharply 2-transitive group is a Frobenius group, results which we obtained for Frobenius groups (Sect. 3.4) apply. In particular, it is easy to show (Exercise 3.4.2) that, for a Frobenius group, $K := \{x \in G \mid x = 1 \text{ or } \mathrm{fix}(x) = \emptyset\}$ is a (normal) subgroup of G if and only if for some $\alpha \in \Omega$, the elements of K lie in distinct right cosets of G_α.

As Example 3.4.3 shows, for a general Frobenius group it is possible that K may be the identity group. However, with the added condition of 2-transitivity we have the following result (see also Theorem 3.4B).

Theorem 7.6D. *Let $G \leq Sym(\Omega)$ be a sharply 2-transitive group, and put $K := \{x \in G \mid x = 1$ or $\mathrm{fix}(x) = \emptyset\}$. Then:*
(i) *G has a unique conjugacy class T of elements of order 2, and each point stabilizer G_α contains at most one element of T;*
(ii) *If for some α the elements of K lie in distinct right cosets of G_α then K is a regular normal abelian subgroup of G.*

PROOF. (i) We first show that for any pair (α, β) of distinct points of Ω, there exists an element of order 2 which interchanges α and β. Indeed by the hypothesis on G, there is a unique element t such that $(\alpha, \beta)^t = (\beta, \alpha)$. Since t^2 fixes both α and β, therefore t has order 2 as required. Now let T denote the conjugacy class of t in G. Suppose that $s \in G$ also has order 2, and that γ and δ are any pair of points interchanged by s. Then we can choose $z \in G$ such that $(\alpha, \beta)^z = (\gamma, \delta)$, and $s^{-1}z^{-1}tz$ fixes both γ and δ. Thus $s^{-1}z^{-1}tz = 1$ and so $s = z^{-1}tz \in T$. This shows that T is the unique conjugacy class of elements of order 2 in G.

Now suppose that $s, t \in T$ both lie in G_α, and pick $\beta \neq \alpha$. Then $\gamma := \beta^s \neq \beta$ and $\delta := \beta^t \neq \beta$. Choose $z \in G$ such that $(\beta, \delta)^z = (\beta, \gamma)$. Then the argument above shows that $s = z^{-1}tz$. Since $\mathrm{fix}(s) = \mathrm{fix}(t) = \{\alpha\}$, this means that z fixes α as well as β, and so $z = 1$. Thus $s = t$, and G_α does not contain more than one element from T.

(ii) We first show that either K contains an element of T or else $TT \subseteq K$. Indeed, if K contains no element from T, then (i) shows that each point stabilizer G_α contains exactly one element from T. In the latter case, any two elements $t, s \in T$ have unique fixed points $\alpha \neq \beta$, respectively, say, and we have to show that $st \in K$. Assume the contrary. Then st also has a unique fixed point γ, say. Since $s^{-1}(st)s = ts = (st)^{-1}$, we have $\{\gamma\} = \mathrm{fix}(st) = \mathrm{fix}((st)^{-1}) = (\mathrm{fix}(st))^s = \{\gamma^s\}$. Thus s fixes γ. Hence $\alpha = \gamma$. Similarly t fixes γ, and so $\beta = \gamma$. Hence $s, t \in G_\gamma$, and so $s = t$ by (i) which is contrary to the assumption that $st \notin K$. Thus we have shown that either K contains an element from T, or $TT \subseteq K$. In particular, $K \neq 1$.

Now the hypothesis on K shows that K is a (nontrivial) subgroup of G, and hence $K \lhd G$ (Exercise 3.4.2). Since G is primitive and K is normal, K must be transitive. Since the point stabilizers of K are trivial, this shows that K is a regular normal subgroup of G.

We finally show that K is abelian. First consider the case where K contains an element of T. Since T is a conjugacy class, and K is normal, this implies that $T \subseteq K$. However, the 2-transitivity of G shows that G_α acts transitively by conjugation on the set $K^\#$ of nonidentity elements of K (Exercise 2.5.5), and so $K^\# = T$. Thus K is a group of exponent 2, and hence an elementary abelian 2-group.

There remains the case where $TT \subseteq$ K. We claim that in this case $K = tT$ for each $t \in T$. Indeed, suppose that α is the unique fixed point of t. For each $x \neq 1$ in K, we can choose $s \in T$ such that α and α^x are interchanged by s (see the proof of (i)). Then $tsx^{-1} \in K$ and fixes α, so $tsx^{-1} = 1$ and $x = ts \in tT$. This proves that $TT \subseteq K \subseteq tT$, and so $K = tT$ as claimed. Now fix $t \in T$ and consider conjugation by t on K. For each $x \in K$ we have $s \in T$ such that $x = ts$ and then $t^{-1}xt = t^{-1}tst = st = s^{-1}t^{-1} = x^{-1}$. Hence conjugation by t inverts the elements of K. In particular, for all $x, y \in K$ we have $xy = t^{-1}(xy)^{-1}t = (t^{-1}y^{-1}t)(t^{-1}x^{-1}t) = yx$. Thus K is abelian in this case as well. □

Exercises

An automorphism τ of a group K is *fixed point free* if $x^\tau \neq x$ for all $x \neq 1$.

7.6.3 Let K be a finite group with a fixed point free automorphism τ of order 2. Show that K is abelian. [*Hint:* Show that each $u \in K$ has the form $x^{-1}x^\tau$ and hence $u^\tau = u^{-1}$.]

7.6.4 Let K be an infinite group with a fixed point free automorphism τ of order 2. Suppose that for each $x \in K$ there is a unique $y \in K$ such that $y^2 = x$. Show that K is abelian. [*Hint:* Show that $y^2 = x^{-1}x^\tau$ implies $y = x^{-1}$.]

7.6.5 Use Exercise 7.6.4 to show that, in the definition of a near field, the commutativity of the group $(F, +)$ in (NF1) can be deduced from the other axioms.

Exercise 7.6.5 shows that the axioms for a near field are at least formally stronger than necessary to define a sharply 2-transitive group. The axioms can be weakened further to define a *near domain.* A near domain is a set F with two binary operations $+$ and $\cdot$ satisfying the following conditions.

ND1: $(F,+)$ has the properties:
- (i) there is a zero element 0 such that $0 + \alpha = \alpha + 0 = \alpha$ for all $\alpha \in F$;
- (ii) $\alpha + \beta = 0 \Rightarrow \beta + \alpha = 0$ for all $\alpha, \beta \in F$;
- (iii) in each equation $\alpha + \beta = \gamma$ any two of the elements determines the third.

ND2: $(F^\#, \cdot)$ is a group where $F^\#$ is the set of nonzero elements of F.

ND3: $\alpha \cdot 0 = 0 \cdot \alpha = 0$ for all $\alpha \in F$.

ND4: For all $\alpha, \beta \in F$ there is an element $\delta_{\alpha,\beta} \in F^\#$ such that $\alpha + (\beta + \gamma) = (\alpha + \beta) + \delta_{\alpha,\beta} \cdot \gamma$.

These conditions are sufficient to define a sharply 2-transitive group (Exercise 7.6.6). A near domain is a near field when the additive structure is a group. The generalization may be formal rather than real: a finite near domain is a near field and it is not known if there are any infinite near domains that are not near fields.

Exercise

7.6.6 Show that if F is a near domain then the mappings $\xi \mapsto \xi \cdot \beta + \alpha$ ($\alpha \in F, \beta \in F^{\#}$) form a sharply 2-transitive group on the set F.

We now consider sharply k-transitive groups with $k \geq 3$. As noted at the begining of this section, Jordan and Tits showed that, apart from the alternating and symmetric groups, M_{11} and M_{12} are the only sharply 4- and 5-transitive groups. On the other hand, there are two easily constructed infinite families of sharply 3-transitive groups of both finite and infinite degrees. Zassenhaus (1936) showed that these two families include all finite sharply 3-transitive groups. The families can be described as follows.

First of all there is the projective general linear group $PGL_2(F)$ acting on the projective line $PG_1(F)$ for an arbitrary field F. As we noted in Sect. 2.8, this group is permutation isomorphic to the group G of all fractional linear mappings of the form

$$t_{\alpha\beta\gamma\delta} : \xi \mapsto \frac{\alpha\xi + \beta}{\gamma\xi + \delta} \quad \text{with } \alpha, \beta, \gamma, \delta \in F \text{ and } \alpha\delta - \beta\gamma \neq 0$$

acting on the set $\Omega := F \cup \{\infty\}$. Note that two of these mappings, $t_{\alpha\beta\gamma\delta}$ and $t_{\alpha'\beta'\gamma'\delta'}$, are equal if and only if the vector $(\alpha', \beta', \gamma', \delta')$ is a nonzero scalar multiple of $(\alpha, \beta, \gamma, \delta)$. It is readily seen that G is 2-transitive on Ω, that G_∞ consists of the mappings $\xi \mapsto \alpha\xi + \beta$ ($\alpha, \beta \in F$ with $\alpha \neq 0$), and that $G_{\infty 0}$ consists of the mappings $\xi \mapsto \alpha\xi$ ($\alpha \in F$ with $\alpha \neq 0$). Since $G_{\infty 0}$ acts regularly on $\Omega \setminus \{\infty, 0\}$, this shows that G is sharply 3-transitive. In the case that F is a finite field of order q, G has order $(q+1)q(q-1)$.

The construction above works for all fields. For some fields it is possible to define a "twisted" version of the construction to obtain a second family of sharply 3-transitive groups. Suppose that F has the properties: F has a field automorphism θ of order 2; and not every element in the multiplicative group $F^{\#}$ of units of F is a square. Then $F^{\#}$ has at least one proper subgroup, say A, such that A contains all the squares in $F^{\#}$ and $A^\theta = A$ (for example, take A as just the set of squares). Consider the mappings

$$s_{\alpha\beta\gamma\delta} : \xi \mapsto \begin{cases} \frac{\alpha\xi+\beta}{\gamma\xi+\delta} & \text{if } \alpha\delta - \beta\gamma \in A \\ \frac{\alpha\xi^\theta+\beta}{\gamma\xi^\theta+\delta} & \text{if } \alpha\delta - \beta\gamma \notin A \end{cases}$$

on $\Omega = F \cup \{\infty\}$ (we extend θ to Ω by defining $\infty^\theta = \infty$). A calculation similar to that just given shows that the set of all $s_{\alpha\beta\gamma\delta}$ ($\alpha, \beta, \gamma, \delta \in F$ with $\alpha\delta - \beta\gamma \neq 0$) forms a group $G(A, \theta)$ which is 3-transitive on Ω (Exercise

7.6.7). The following examples are cases where the underlying field has the appropriate properties.

EXAMPLE 7.6.3. If F is a finite field of size q, then F has the appropriate properties only in the case that q is a square (so $|\mathrm{Aut}(F)|$ is even) and q is odd (so the squares form a subgroup of index 2 in the group of units). Conversely, suppose that q is an odd prime power, and that q is a square, say $q = r^2$. Then we can take $F := \mathbb{F}_q$, $\theta : \xi \mapsto \xi^r$ and A as the set of all nonzero squares in F. Then the construction above gives a sharply 3-transitive group of order $(q+1)q(q-1)$ which is not permutation isomorphic to $PGL_2(q)$ acting on Ω (see Exercise 7.6.8).

EXAMPLE 7.6.4. Let $F := \mathbb{Q}[i]$ be the field obtained by adjoining the complex square root of 1 to the rational field. Then complex conjugation gives an automorphism θ of order 2 for F. For each (rational) prime p, and for each $\alpha \neq 0$ in F define $\nu_p(\alpha)$ to be the exponent of p in the canonical factorization of the rational number $|\alpha|^2$. Let Π be any nonempty set of primes. Then $A_\Pi := \{\alpha \in F \mid \alpha \neq 0, \nu_p(\alpha) \text{ even for all } p \in \Pi\}$ is a subgroup of the group of units of F which is obviously fixed by θ and contains all the squares. The construction above gives a sharply 3-transitive group $G(A_\Pi, \theta)$ acting on $PG_1(F) = F \cup \{\infty\}$.

EXAMPLE 7.6.5. Let $F := K(X)$ be the field of all rational functions over an arbitrary field K. Each nonzero $f \in F$ has the form f_1/f_2 for some polynomials f_1, f_2 in $K[X]$; we define $\nu(f) := \deg f_1 - \deg f_2$ and put $A := \{f \in F \mid f \neq 0 \text{ and } \nu(f) \text{ even }\}$. Then A is a subgroup of index 2 in the group of units of F. There are several ways to define an automorphism θ of order 2 for F mapping A onto itself. Two examples are:
(i) θ fixes every element of K and maps $X \mapsto 1 - X$;
(ii) θ fixes X and acts as an automorphism of order 2 on K.

Exercises

7.6.7 Show that the group $G(A, \theta)$ defined in the "twisted" version of the construction is sharply 3-transitive on $\Omega = F \cup \{\infty\}$.

7.6.8 For $\alpha \in F^\#$, let $x_\alpha := s_{\alpha 010} \in (G(A, \theta))_{\infty 0}$.
  (i) Show that $x_\alpha x_\beta \neq x_\beta x_\alpha$ whenever $\alpha \in A$ and $\beta \notin A$.
  (ii) Hence show that $G(A, \theta)$ is not permutation isomorphic to $PGL_2(F)$ acting on $PG_1(F)$.

7.7 The Finite 2-transitive Groups

This is a largely expository section in which we shall describe the complete list of finite 2-transitive groups, although we shall not prove that

this list is complete. We know from Theorem 4.1B that the socle of any finite 2-transitive group is either elementary abelian or else a primitive simple group, and this explains the direct relationship between classifying finite 2-transitive groups and classifying finite simple groups. A detailed examination of possible cases was carried out by a number of different mathematicians in anticipation of the classification of finite simple groups, and led to the results described here.

There are eight infinite families of finite 2-transitive groups. These include the familiar cases of the alternating, symmetric, affine and projective groups (in their natural actions). The less familiar ones are groups of Lie type: the symplectic groups $Sp_{2m}(2)$, the Suzuki groups $Sz(q)$, the unitary groups $PGU_3(q^2)$, and the Ree groups $R(q)$. The symplectic groups each have two distinct 2-transitive actions. Each of the groups from the other three classes is 2-transitive on the set of points in its action on an appropriate Steiner system. In addition to these eight infinite families, there are ten exceptional (sporadic) examples of 2-transitive groups. We describe all these groups in more detail below.

Alternating and symmetric groups

These are the trivial examples. In their natural actions, S_d is d-transitive and A_d is $(d-2)$-transitive. In only a few cases, covered below, are they 2-transitive in any other action (see Exercise 7.7.1).

Exercise

7.7.1 If $n > 7$, show that neither A_n nor S_n has a 2-transitive representation of degree $> n$. [*Hint:* If G acts on Ω, and C is a conjugacy class for G, then α^C is G_α-invariant for any $\alpha \in \Omega$.]

Affine groups

A 2-transitive group with abelian socles is permutation isomorphic to a subgroup of $A\Gamma L_d(q)$ for some d and q, and has degree q^d. Conversely, a subgroup $G \leq A\Gamma L_d(q)$ is 2-transitive if and only if the point stabilizer $G_0 \leq \Gamma L_d(q)$ acts transitively on the set of nonzero vectors in the underlying vector space. The 2-transitive solvable groups have been determined by Huppert (1957), and the 2-transitive nonsolvable affine groups have been determined by Hering (1974) [see also Huppert and Blackburn (1982) XII §7.5]. Each of the latter has a unique nonabelian composition factor. There are three infinite families of examples :

(i) $SL_d(q) \leq G_0 \leq \Gamma L_d(q)$;
(ii) $Sp_d(q) \leq G_0 \leq \Gamma L_d(q)$; and
(iii) $G_0 = G_2(2^m) \leq \Gamma L_6(2^m)$.

In addition there is a small number of sporadic examples of dimensions 2, 4 and 6. Some of these appear in Sect. 7.6 as sharply 2-transitive groups.

Two further examples can be found in Exercises 7.7.15 and 7.7.16 (if we identify $PG_4(2)$ and $\mathbb{F}_2^4$).

Projective groups $PSL_d(q)$

The projective groups are defined in Sect. 2.8. The group $PSL_d(q)$ has a faithful 2-transitive action of degree $(q^d - 1)/(q - 1)$ on $\Omega := PG_d(q)$ (or, equivalently, on the set of 1-dimensional subspaces of $\mathbb{F}_q$). Apart from the cases $(d, q) = (2, 2)$ or (2,3), $PSL_d(q)$ is a nonabelian simple group. The normalizer of $PSL_d(q)$ in $Sym(\Omega)$ is $P\Gamma L_d(q)$ which is generated by $PGL_d(q)$ together with the permutations induced by the field automorphisms of $\mathbb{F}_q$.

In the case $d = 2$, $PGL_2(q)$ is sharply 3-transitive of degree $q + 1$, and so $P\Gamma L_2(q)$ is also 3-transitive. Note that $PSL_2(q) = PGL_2(q)$ if q is even but that $PSL_2(q)$ has index 2 in $PGL_2(q)$ when q is odd. Also, as abstract groups, $PSL_2(4) \cong PSL_2(5) \cong A_5$, $PSL_2(7) \cong PSL_3(2)$, $PSL_2(9) \cong A_6$ and $PSL_4(2) \cong A_8$.

The symplectic groups $Sp_{2m}(2)$

Let F be an arbitrary field, $m \geq 1$ a fixed integer, and let $V := F^{2m}$. We define two block matrices over F of the form

$$e := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad f := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = e - e^{\mathrm{T}}$$

where 0 and 1 denote the $m \times m$ zero and identity matrices, respectively, (and e^{T} denotes the transpose of e). Then $Sp_{2m}(F)$ is the subgroup of $GL_{2m}(F)$ consisting of all matrices x such that $xfx^{\mathrm{T}} = f$. When F is a finite field of size q, it is known that $|Sp_{2m}(F)| = q^{m^2} \prod_{i=1}^{m}(q^i - 1)$ [see Taylor (1974)].

Associated with f is the symmetric bilinear form $\varphi : V \times V \to F$ defined by $\varphi(u, v) := ufv^{\mathrm{T}}$. If the characteristic of F is not 2, then there is a natural way to associate a quadratic form to every bilinear form. Namely, using a suitable scaling, we can take the quadratic form θ to be $\theta(u) := \frac{1}{2}\varphi(u, u)$; and φ can be recovered from θ by use of the "polarization identity"

$$\text{(7.4)} \qquad \varphi(u, v) = \theta(u + v) - \theta(u) - \theta(v) \quad \text{for all } u, v \in V.$$

Thus, when char $F \neq 2$, there is a one-to-one correspondence between bilinear forms and quadratic forms. If char $F = 2$ (which is the case we are interested in), this correspondence no longer exists, and often, for a general bilinear form, there will be no quadratic form satisfying the polarization identity. For the bilinear function φ defined above, however, it can be easily verified that, in characteristic 2, the quadratic form $\theta = \theta_0(u) := ueu^{\mathrm{T}}$ ($= ue^{\mathrm{T}}u^{\mathrm{T}}$) satisfies condition (7.4).

Now suppose char $F = 2$ and consider the set Ω of all functions $\theta : V \to F$ such that condition (7.4) is satisfied for our particular bilinear form $\varphi(u, v) = ufv^{\mathrm{T}}$. Since $\theta_0 \in \Omega$, we have $\theta \in \Omega$, if and only if the

function $\lambda := \theta - \theta_0$ satisfies $\lambda(u+v) = \lambda(u) + \lambda(v)$ for all $u, v \in V$ (and so λ is a homomorphism of the group $(V, +)$ into $(F, +)$).

From now on we specialize to the case where $F = \mathbb{F}_2$. Then each group homomorphism of $(V, +)$ into $(F, +)$ is an F-linear transformation, and so has the form $\lambda(u) = uc^{\mathrm{T}}$ for some $c \in V$. Since f is invertible we can replace c^{T} by fa^{T}, and so conclude that $\Omega = \{\theta_a \mid a \in V\}$ where

$$(7.5) \qquad \theta_a(u) := ueu^{\mathrm{T}} + ufa^{\mathrm{T}} = \theta_0(u) + \varphi(u, a).$$

For later purposes note that, since $F = \mathbb{F}_2$, therefore $f = e + e^{\mathrm{T}}$ and the values of θ_a and φ are always 0 or 1.

Now put $G := Sp_{2m}(2)$ $(= Sp_{2m}(\mathbb{F}_2))$. Since G acts on V and leaves f invariant, the definition of Ω shows that G also acts in a natural way on Ω where for $x \in G$ and $\theta \in \Omega$ we have $\theta^x(u) := \theta(ux^{-1})$ (see Sect. 2.6). Our object is to show that Ω can be partitioned into two G-invariant subsets such that G acts 2-transitively on each of these sets.

We begin by defining the transvections $t_a : V \to V$ given by $ut_a := u + \varphi(u, a)a$ for each $a \in V$. It is readily seen that each t_a lies in G, that $t_a = t_a$, and that $x^{-1}t_a x = t_{ax}$ for all $x \in G$ (see Exercise 7.7.5). Using equation (7.4) and the fact that $\varphi(u, c) = 0$ or 1, we have the identity

$$(7.6) \quad \theta_a^{t_c}(u) = \theta_a(ut_c^{-1}) = \theta_a(u + \varphi(u, c)c) = \theta_a(u) + (\theta_a(c) + 1)\varphi(u, c).$$

Lemma 7.7A.

(i) *For all $a, c \in V$ we have*

$$\theta_a^{t_c} = \begin{cases} \theta_a & \text{if } \theta_a(c) = 1 \\ \theta_{a+c} & \text{if } \theta_a(c) = 0 \end{cases}.$$

(ii) *For all $a, b \in V$ there is at most one $c \in V$ such that t_c maps θ_a onto θ_b. Such a c exists if and only if $\theta_0(a) = \theta_0(b)$ (and then $c = a + b$).*

PROOF. (i) When $\theta_a(c) = 1$, this follows immediately from equations (7.5) and (7.6). When $\theta_a(c) = 0$, we have $\theta_a^{t_c}(u) = \theta_a(u) + \varphi(u, c) = \theta_0(u) + \varphi(u, a) + \varphi(u, c) = \theta_0(u) + \varphi(u, a + c) = \theta_{a+c}(u)$.

(ii) It follows at once from (i) that there is at most one c such that t_c maps θ_a onto θ_b; namely, $c = a + b$. Moreover, this value of c has the required property if and only if $\theta_a(a + b) = 0$. However, using equation (7.4) and the fact that $\varphi(a, a)$ is always 0, we have

$$\theta_a(a + b) = \theta_a(a) + \theta_a(b) + \varphi(a, b) = \theta_0(a) + \theta_0(b)$$

and so the result follows. □

We now define $H := \langle t_a \mid a \in V \rangle \leq G$. Exercise 7.7.5 shows that H is normal in G. It is known that $G' = G = H$ whenever $m \geq 3$, but we shall not need that fact here [see Taylor (1974)].

Corollary 7.7A. *H has two orbits on* Ω, *namely*

$$\Omega^+ := \{\theta_a \mid \theta_0(a) = 0\} \quad \textit{and} \quad \Omega^- := \{\theta_a \mid \theta_0(a) = 1\}$$

with $|\Omega^+| = 2^{m-1}(2^m + 1)$ *and* $|\Omega^-| = 2^{m-1}(2^m - 1)$. *These are also orbits for* $G = Sp_{2m}(2)$.

PROOF. The first assertion follows at once from part (ii) of the lemma and Exercise 7.7.6. The second assertion follows from the observation that otherwise G would be transitive, and this is impossible because the orbits of the normal subgroup H have different sizes (Theorem 1.6A). □

Our main theorem will show that H (and hence G) acts 2-transitively on each of these orbits. We isolate part of the argument in the following lemma. For each nonzero vector $a \in V$ and $\epsilon \in \mathbb{F}_2$ we define $L(a, \epsilon) = \{v \in V \mid \varphi(v, a) = \epsilon\}$. Thus $L(a, \epsilon)$ is an affine subspace of dimension $2m - 1$ in V. If $a_1, \ldots, a_k$ are linearly independent, then the conditions $\varphi(v, a_i) = \epsilon_i$ $(i = 1, \ldots, k)$ are equivalent to a system of k linear equations of rank k on the entries of V. Hence, by elementary linear algebra, $\bigcap_{i=1}^{k} L(a_i, \epsilon_i) = U + w_0$ for some subspace U of dimension $2m - k$ in V and some $w_0 \in V$. We have $w_0 = 0$ when all $\epsilon_i = 0$.

Lemma 7.7B. *Let* $m \geq 3$. *Then* θ_0 *is not constant on* $L(a, \epsilon_1) \cap L(b, \epsilon_2)$ *whenever* a *and* b *are distinct elements in* V *and* $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$.

PROOF. Since $\mathbb{F}_2$ has only two elements, $a \neq b$ implies that a and b are linearly independent. Hence $U := L(a, 0) \cap L(b, 0)$ is a subspace of dimension $2m - 2 > 2$ in V, and so contains an element c which is linearly independent of a and b. Thus there exists $w \in L(a, \epsilon_1) \cap L(b, \epsilon_2) \cap L(c, \epsilon_3)$ for any $\epsilon_3 \in \mathbb{F}_2$. By the choice of c, both w and $w + c$ lie in $L(a, \epsilon_1) \cap L(b, \epsilon_2)$. On the other hand, $\theta_0(w + c) = \theta_0(w) + \theta_0(c) + \varphi(w, c) = \theta_0(w) + \theta_0(c) + \epsilon_3$. Hence we can choose $\epsilon_3 = \theta_0(c) + 1$ to ensure that $\theta_0(w + c) \neq \theta_0(w)$. This proves the lemma. □

Theorem 7.7A. $Sp_{2m}(2)$ *acts 2-transitively on each of the orbits* Ω^+ *and* Ω^- *for each* $m \geq 2$.

PROOF. We shall prove the theorem only for $m \geq 3$. The case where $m = 2$ is left as an exercise (see Exercises 7.7.7 and 7.7.8).

We know that Ω^+ and Ω^- are both orbits for G (and H), so it is enough to show that H acts 2-transitively on each of them. Equivalently, we shall show that, if $\epsilon \in \mathbb{F}_2$, and $a, b, c \in V$ satisfy $\theta_0(a) = \theta_0(b) = \theta_0(c) = \epsilon$, then there is an element $x \in H$ which maps θ_a onto θ_b leaving θ_c fixed (this shows that the point stabilizer of θ_c in H is transitive on the remaining points of the orbit containing θ_c). More precisely, we shall show that under these hypotheses on a, b and c, there exists $w \in \Omega$ such that:

$$\theta_0(w) = \epsilon \quad \text{and} \quad \theta_c(a + w) = \theta_c(b + w) = 1. \tag{7.7}$$

Then Lemma 7.7A(ii) shows that $x = t_{a+w}t_{b+w}$ has the required property.

It remains to show that there exists w satisfying (7.7). First note that $\theta_c(a+w) = \theta_c(a) + \theta_c(w) + \varphi(w,a) = \theta_0(a) + \theta_0(w) + \varphi(a,c) + \varphi(w,c) + \varphi(w,a)$, with a similar expansion for $\theta_c(b+w)$. Therefore the conditions (7.7) are equivalent to

$$(7.8)\quad \varphi(w, a+c) = 1 + \varphi(a,c), \varphi(w, b+c) = 1 + \varphi(b,c) \text{ and } \theta_0(w) = \epsilon.$$

Finally, the set of $w \in V$ satisfying the first two equations in (7.8) is simply $L(a+c, 1+\varphi(a,c)) \cap L(b+c, 1+\varphi(b,c))$, and Lemma 7.7B shows that θ_0 is not constant on this set. Thus, whatever value ϵ takes, there exists w satisfying all the conditions of (7.8) as required. □

Exercises

7.7.2 Show that $Sp_2(F) = SL_2(F)$ for any field F.

7.7.3 For any field F, prove that all matrices of the form

$$\begin{bmatrix} a^{-1} & 0 \\ 0 & a^{\mathrm{T}} \end{bmatrix}, \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} \quad \text{with } b = b^{\mathrm{T}}$$

(where all blocks are $m \times m$ over F) lie in $Sp_{2m}(F)$. Characterize more precisely the elements of $Sp_{2m}(F)$.

In the remaining exercises it is assumed that $F = \mathbb{F}_2, G = Sp_{2m}(2)$ and H is the subgroup generated by transvections.

7.7.4 Show that each function θ in Ω can be written as a quadratic form (when $F = \mathbb{F}_2$).

7.7.5 Show that for all $a \in V$ and all $x \in G$, t_a has order 2 and $x^{-1}t_a x = t_{ax}$. In particular, the latter shows that $H \lhd G$.

7.7.6 Show that the orbits Ω^+ and Ω^- of G have sizes $2^{m-1}(2^m+1)$ and $2^{m-1}(2^m-1)$, respectively.

7.7.7 When $m = 2$, show that $G = Sp_4(2) \cong S_6$, and $H \cong A_6$.

7.7.8 Prove Theorem 7.7A in the case $m = 2$.

7.7.9 Show that, for each $m \geq 2$, the group G acts faithfully on each of the orbits Ω^+ and Ω^-.

Unitary groups, $U_3(q)$

Let q be a power of a prime and let $K := \mathbb{F}_{q^2}$. Denote by V the 3-dimensional vector space over K. The mapping $\sigma : \xi \mapsto \xi^q$ is an automorphism of K and $\sigma^2 = 1$. This automorphism of order 2 allows us to define a hermitian form $\varphi : V \times V \to K$. Thus, for all $u, v \in V$ and $\alpha, \beta \in K$ we have $\varphi(\alpha u, \beta v) = \alpha\beta^q \varphi(u,v)$ and $\varphi(u,v) = \varphi(v,u)^q$. The *unitary group* $GU_3(q)$ is the subgroup of $GL_3(q^2)$ that preserves φ. So $h \in GL_3(q^2)$ is an element of $GU_3(q) \iff \varphi(u,v) = \varphi(u^h, v^h)$ for all $u, v \in V$. The group $GU_3(q)$ induces an action on the 1-dimensional subspaces of V; the induced group is the *projective unitary group*, $PGU_3(q)$,

a subgroup of the projective general linear group $PGL_3(q^2)$. The group $PGU_3(q)$ has a subgroup $PSU_3(q) = PGU_3(q) \cap PSL_3(q^2)$ and can be extended to a group $P\Gamma U_3(q)$ by adding the field automorphisms (by analogy with the group $P\Gamma L_3(q^2)$). In fact, $PSU_3(q)$ is a proper subgroup of $PGU_3(q)$ only if 3 divides $q+1$, in which case the index is 3. If $q > 2$ then the group $PSU_3(q)$ is simple.

Any vector $u \in V$ such that $\varphi(u,u) = 0$ is called *isotropic*. Clearly, the elements of $PGU_3(q)$ leave the set of isotropic vectors invariant. Every scalar multiple of an isotropic vector is again isotropic so the set of 1-dimensional subspaces $\Omega = \{\langle u\rangle \mid \varphi(u,u) = 0\}$ is invariant under the action of $PGU_3(q)$ (actually it is invariant under all of $P\Gamma L_3(q)$). This is the action of interest; the group $PSU_3(q)$ is 2-transitive on the set Ω.

By taking a specific bilinear form φ we can describe this 2-transitive action in more detail. Let $u = (\xi_1, \xi_2, \xi_3)$, $v = (\eta_1, \eta_2, \eta_3)$ be variables defined on V. Using $\xi \mapsto \overline{\xi} = \xi^q$ to denote the automorphism of order 2, we take $\varphi(u,v) = \xi_1\overline{\eta_3} + \xi_3\overline{\eta_1} + \xi_2\overline{\eta_2}$. It is straightforward to calculate that for this choice of bilinear form the set of 1-dimensional isotropic subspaces is

$$\Omega = \{\langle(1,0,0)\rangle\} \cup \{\langle(\alpha,\beta,1)\rangle \mid \alpha + \overline{\alpha} + \beta\overline{\beta} = 0, \alpha, \beta \in \mathbb{F}_{q^2}\}.$$

Thus $|\Omega| = q^3 + 1$.

We can also give a simple description of some of the elements of the group $G = PGU_3(q)$ corresponding to this choice of bilinear form. Define

$$t_{\alpha,\beta} = \begin{bmatrix} 1 & -\overline{\beta} & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{bmatrix} \text{ and } h_{\gamma,\delta} = \begin{bmatrix} \gamma & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & \overline{\gamma}^{-1} \end{bmatrix}.$$

These define elements of G, to which we give the same names, if $\alpha, \beta, \gamma, \delta$ are elements of $\mathbb{F}_{q^2}$ and also $\delta\overline{\delta} = 1$, $\gamma \neq 0$, $\alpha + \overline{\alpha} + \beta\overline{\beta} = 0$. There are q^3 matrices of the type $t_{\alpha,\beta}$ and $(q^2-1)(q+1)$ of type $h_{\gamma,\delta}$. Let $e_1 = (1,0,0)$ and $e_3 = (0,0,1)$. Then the stabilizer $G_{\langle e_1\rangle}$ of the subspace spanned by e_1 consists of the elements represented as $x = h_{\gamma,\delta}t_{\alpha,\beta}$ (where $\delta\overline{\delta} = 1$, $\gamma \neq 0$, $\alpha + \overline{\alpha} + \beta\overline{\beta} = 0$). The set $T = \{t_{\alpha,\beta} \mid \alpha + \overline{\alpha} + \beta\overline{\beta} = 0\}$ is a normal subgoup of $G_{\langle e_1\rangle}$ acting regularly on $\Omega \setminus \{\langle e_1\rangle\}$. Since there are elements of G that do not fix $\langle e_1\rangle$ (Exercise 7.7.10), it follows that G is 2-transitive. Since the matrices $t_{\alpha,\beta}$ clearly have determinant 1, the group $PSU_3(q)$ is similarly 2-transitive on Ω. The stabilizer in GU of the two points $\langle e_1\rangle$ and $\langle e_3\rangle$ of Ω is $GU_{\langle e_1\rangle\langle e_3\rangle} = \{h_{\gamma,\delta} \mid \gamma \neq 0, \delta\overline{\delta} = 1\}$. The element $h_{\gamma,\delta}$ is a scalar matrix, and hence acts trivially on Ω, if $\gamma = \delta$ and $\delta\overline{\delta} = 1$. Thus the group $G_{\langle e_1\rangle\langle e_3\rangle}$ has order $q^2 - 1$.

The unitary group $U_3(q)$ acts as a group of automorphisms of a certain combinatorial geometry. As points of this geometry we take the set Ω of 1-dimensional isotropic subspaces. A plane containing more than one isotropic subspace must contain $q+1$ such subspaces (Exercise 7.7.12); these sets of points are the blocks of the geometry. This system of points

and blocks is an $S(2, q+1, q^3+1)$ Steiner system. Such a Steiner system is called a *unital*.

For further details on the unitary groups see O'Nan (1973) and Taylor (1974) and (1992).

Exercises

7.7.10 For the particular choice of bilinear form above, find an element of $PSU_3(q)$ that does not fix $< e_1 >$.

7.7.11 Define $t : V \to V$ by $t : v \mapsto v + a\varphi(v, u) \cdot u$ where $a + \bar{a} = 0$ and u is isotropic. Show that t is an element of $GU_3(q)$. Such an element is called a *unitary transvection*; these elements generate $PSU_3(q)$ if $q > 2$.

7.7.12

(i) Suppose that u, v are isotropic and that $\varphi(u, v) = 1$. Show that the vector $u + \alpha v$ is isotropic $\iff \alpha + \bar{\alpha} = 0$.

(ii) Show that there are $q + 1$ solutions of $\alpha + \bar{\alpha} = \alpha + \alpha^q = 0$ in $\mathbb{F}_{q^2}$.

Suzuki groups

The group Suzuki group $Sz(q)$, which is also called ${}^2B_2(q)$, is defined when $q = 2^{2m+1}$ is an odd power of two. The group has order $(q^2+1)q^2(q-1)$ and is simple if $q > 2$. (The group $Sz(2) \cong AGL_1(5)$.) It is an automorphism group of an S$(3, q+1, q^2+1)$ Steiner system (an inversive plane of order q). The group $Sz(q)$ is 2-transitive on the $q^2 + 1$ points and a stabilizer of two points is cyclic. Let $K := \mathbb{F}_q$. To define the group $Sz(q)$ we consider the automorphism $\sigma \in \mathrm{Aut}(K)$ defined by $\sigma\colon \xi \mapsto \xi^{2^{m+1}}$. Since $q = 2^{2m+1}$, σ^2 is the Frobenius automorphism $\xi \mapsto \xi^2$.

Define $\Omega := \{(\eta_1, \eta_2, \eta_3) \in K^3 \mid \eta_3 = \eta_1\eta_2 + \eta_1^{\sigma+2} + \eta_2^{\sigma}\} \cup \{\infty\}$. Thus $|\Omega| = q^2+1$. For $\alpha, \beta, \kappa \in K$ with $\kappa \neq 0$, define the following permutations of Ω fixing ∞:

$$\begin{aligned} t_{\alpha,\beta}\colon (\eta_1, \eta_2, \eta_3) \mapsto\ & (\eta_1 + a, \eta_2 + b + a^{\sigma}\eta_1, \\ & \eta_3 + ab + a^{\sigma+2} + b^{\sigma} + a\eta_2 + a^{\sigma+1}\eta_1 + b\eta_1) \\ n_{\kappa}\colon (\eta_1, \eta_2, \eta_3) \mapsto\ & (\kappa\eta_1, \kappa^{\sigma+1}\eta_2, \kappa^{\sigma+2}\eta_3) \end{aligned}$$

Finally, define the involution w fixing Ω by

$$w : (\eta_1, \eta_2, \eta_3) \leftrightarrow \left(\frac{\eta_2}{\eta_3}, \frac{\eta_1}{\eta_3}, \frac{1}{\eta_3}\right) \quad \text{for } \eta_3 \neq 0,$$
$$\infty \leftrightarrow (0, 0, 0)$$

The Suzuki group $Sz(q)$ is the group generated by w and all $t_{\alpha,\beta}, n_{\kappa}$. The stabilizer of ∞ is $Sz(q)_{\infty} = \langle t_{\alpha,\beta}, n_{\kappa} \mid \alpha, \beta, \kappa \in K, \kappa \neq 0\rangle$. The stabilizer of the two points ∞ and $(0,0,0)$ is the cyclic group $\langle n_{\kappa} \mid \kappa \in K^{\#}\rangle$. The subgroup $T := \langle t_{\alpha,\beta} \mid \alpha, \beta \in K\rangle$ is a Sylow 2-subgroup and is a normal subgroup of $Sz(q)_{\infty}$ acting regularly on $\Omega \setminus \{\infty\}$. Since w does not fix

∞ it follows that $Sz(q)$ is 2-transitive on Ω. For complete details on the definition and structure of the Suzuki groups see Suzuki (1960) and (1962), Tits (1960) and (1962) or Lüneburg (1980).

Exercises

7.7.13 Assuming that the set of permutations $T = \{t_{\alpha,\beta} \mid \alpha, \beta \in K\}$ is closed under composition, show that T is transitive on $\Omega \setminus \{\infty\}$ and is normalized by n_κ for all $\kappa \in K^{\#}$.

7.7.14 Show that the permutation $t_{\alpha,\beta} \neq 1$ has order 4 if $\alpha \neq 0$ and has order 2 if $\alpha = 0$.

Ree groups

The Ree groups can be defined in a way that parallels the description of the Suzuki groups above. The Ree group $R(q)$, which is also called ${}^2G_2(q)$, is defined when $q = 3^{2m+1}$ is an odd power of 3 and has order $(q^3+1)q^3(q-1)$. The group $R(q)$ is simple if $q > 3$; the group $R(3) \cong P\Sigma L_2(8)$ has a normal subgroup of index 3. The group $R(q)$ acts as an automorphism group of an $S(2\ , q+1, q^3+1)$ Steiner system (a unital of order q). $R(q)$ is 2-transitive on the q^3+1 points and the stabilizer of two points is cyclic. Let $K := \mathbb{F}_q$. To define the group $R(q)$ we use an automorphism $\sigma \in \operatorname{Aut}(K)$ defined by $\sigma\colon \xi \mapsto \xi^{3^{m+1}}$. Since $q = 3^{2m+1}$, σ^2 is the Frobenius automorphism $\xi \mapsto \xi^2$.

The set Ω of points on which $R(q)$ acts consists of ∞ and the set of sixtuples $(\eta_1, \eta_2, \eta_3, \lambda_1, \lambda_2, \lambda_3)$ with $\eta_1, \eta_2, \eta_3 \in K$ and

$$\begin{aligned}
\lambda_1 &= \eta_1^2\eta_2 - \eta_1\eta_3 + \eta_2^\sigma - \eta_1^{\sigma+3}\\
\lambda_2 &= \eta_1^\sigma\eta_2^\sigma - \eta_3^\sigma + \eta_1\eta_2^2 + \eta_2\eta_3 - \eta_1^{2\sigma+3}\\
\lambda_3 &= \eta_1\eta_3^\sigma - \eta_1^{\sigma+1}\eta_2 + \eta_1^{\sigma+3}\eta_2 + \eta_1^2\eta_2^2 - \eta_2^{\sigma+1} - \eta_3^2 + \eta_1^{2\sigma+4}.
\end{aligned}$$

Thus $|\Omega| = q^3 + 1$. For $\alpha, \beta, \gamma, \kappa \in K$ with $\kappa \neq 0$, define the following permutations of Ω fixing ∞:

$$\begin{aligned}
&t_{\alpha,\beta,\gamma}\colon (\eta_1, \eta_2, \eta_3, \lambda_1, \lambda_2, \lambda_3) \mapsto\\
&\quad (\eta_1 + \alpha, \eta_2 + \beta + \alpha^\sigma\eta_1, \eta_3 + \gamma - \alpha\eta_2 + \beta\eta_1 - \alpha^{\sigma+1}\eta_1, \ldots, \ldots, \ldots)\\
&n_\kappa\colon (\eta_1, \eta_2, \eta_3, \lambda_1, \lambda_2, \lambda_3) \mapsto\\
&\quad (\kappa\eta_1, \kappa^{\sigma+1}\eta_2, \kappa^{\sigma+2}\eta_3, \kappa^{\sigma+3}\lambda_1, \kappa^{2\sigma+3}\lambda_2, \kappa^{2\sigma+4}\lambda_3).
\end{aligned}$$

(The missing formulas in the definition of $t_{\alpha,\beta,\gamma}$ are long and can be calculated from the formulas given and the fact that $t_{\alpha,\beta,\gamma}$ leaves Ω invariant.) Finally, define the involution w fixing Ω by

$$(\eta_1, \eta_2, \eta_3, \lambda_1, \lambda_2, \lambda_3) \leftrightarrow \left(\frac{-\lambda_2}{\lambda_3}, \frac{-\lambda_3}{\lambda_3}, \frac{-\eta_3}{\lambda_3}, \frac{-\eta_2}{\lambda_3}, \frac{-\eta_1}{\lambda_3}, \frac{1}{\lambda_3}\right)$$

for $\lambda_3 \neq 0$ and

$$\infty \leftrightarrow (0, 0, 0, 0, 0, 0).$$

The Ree group $R(q)$ is the group generated by w and all $t_{\alpha,\beta,\gamma}, n_\kappa$. The stabilizer of ∞ is $R(q)_\infty = \langle t_{\alpha,\beta,\gamma}, n_\kappa \mid \alpha, \beta, \gamma, \kappa \in K, \kappa \neq 0\rangle$. The stabilizer of the two points ∞ and $(0,0,0)$ is the cyclic group $\langle n_\kappa \mid \kappa \in K^\#\rangle$. The subgroup $T := \langle t_{\alpha,\beta,\gamma} \mid \alpha, \beta \in K\rangle$ is a Sylow 3-subgroup and is a normal subgroup of $R(q)_\infty$ acting regularly on $\Omega \setminus \{\infty\}$. Since w does not fix ∞ it follows that $R(q)$ is 2-transitive on Ω. For more details on the definition and structure of the Ree groups see Tits (1960), Ree (1961) or Huppert and Blackburn (1982).

The previous 2-transitive groups all fell into infinite classes. The remaining ten groups are the sporadic 2-transitive groups.

Mathieu groups

The five Mathieu groups were constructed in Chap. 6. The groups M_{12} and M_{24} are the only nontrivial finite 5-transitive groups while M_{11} and M_{23} are the only nontrivial finite 4-transitive groups.

$PSL_2(11)$ and M_{11}

We showed in Chap. 6 that the 24 points on which M_{24} acts can be partitioned into two sets Δ, Γ of 12 points each such that the set stabilizer of Δ is the Mathieu group M_{12}. The stabilizer in this latter group of a point in Δ is isomorphic to M_{11} and acts 3-transitively on the 12 points of Γ. The point stabilizer in this action of degree 12 is $PSL_2(11)$ acting 2-transitively on 11 points. These actions were also constructed, using transitive extensions, in Example 7.5.2.

$A_7 < PGL_4(2)$

The 3-dimensional projective space $PG_3(2)$ has 15 points and admits the automorphism group $PGL_4(2)$. It was shown in Exercise 6.8.10 that $A_8 \cong PSL_4(2)$. Therefore there is a subgroup G of $PSL_4(2)$ of index 8 isomorphic to A_7. It happens that this subgroup G acts 2-transitively on the 15 points.

Exercises

7.7.15 Prove that the subgroup $G \cong A_7$ of $PSL_2(4)$ acts 2-transitively on $PG_3(2)$.

7.7.16 (Continuation) Show that a subgroup of A_7 isomorphic to A_6 is transitive on $PG_3(2)$.

The Higman–Sims group

The Higman–Sims group HS is one of the sporadic finite simple groups; it has order 44,352,000 (see Appendix A). The group HS can be described as the automorphism group of a combinatorial geometry consisting of a set Ω of 176 points and a set Γ of 176 quadrics such that each quadric consists of 50 points and each point is in 50 quadrics. Each pair of points (respectively, quadrics) is incident with exactly 14 quadrics (respectively points) giving

a symmetric 2-(176,50,14) design. The group HS is 2-transitive in its action on Ω and has an equivalent 2-transitive action on Γ. This particular combinatorial geometry can be constructed from the Witt geometry W_{24} (see Chap. 6); for details see Higman (1969) or Smith (1976).

The Higman–Sims group also has a rank 3 permutation action on a set of 100 points. The Higman–Sims graph $\mathcal{H}$ is a graph with 100 vertices built from the Witt geometry W_{22} for the Mathieu group M_{22}. The vertex set of $\mathcal{H}$ consists of the 22 points and the 77 blocks of W_{22} as well as one additional vertex ω. The vertex ω is joined in $\mathcal{H}$ to each point of W_{22}, each point of W_{22} is joined to each of the blocks of W_{22} that contain the point, and two blocks of W_{22} are joined when they are disjoint. Each vertex of the resulting graph has degree 22. Clearly M_{22} acts as an automorphism group of $\mathcal{H}$ fixing ω. The full automorphism group of $\mathcal{H}$ is the automorphism group $HS.2$ of the Higman–Sims group. For further details see Higman and Sims (1968), Biggs and White (1979), or Beth et al. (1993).

The Conway group Co_3

The group Co_3 is a sporadic simple group of order $2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 =$ 495,766,656,000. It is closely related to the Higman–Sims group but is most naturally defined using a different combinatorial structure. A *lattice* in $\mathbb{R}^n$ is a subset consisting of all integral linear combinations of some basis of $\mathbb{R}^n$. The automorphisms of the lattice are the linear transformations of $\mathbb{R}^n$ that fix the lattice setwise. The *Leech Lattice* Λ is a particular, and quite exceptional, 24-dimensional lattice which can be constructed using the Witt geometry W_{24}, the S(2,8,24) Steiner system constructed in Chap. 6. Many interesting groups occur as subgroups of $\mathrm{Aut}(\Lambda)$ fixing particular types or configurations of vectors in Λ. In particular, the group Co_3 is the stabilizer of a vector of "type 3". This group has a 2-transitive action of degree 276 also derived from the lattice. The stabilizer of a point in this action is $McL : 2$, the automorphism group of the McLaughlin group which is also a sporadic simple group. Furthermore, Co_3 has a subgroup isomorphic to the Higman–Sims group HS which has two orbits: one of length 100, the other of length 176. The actions of HS on these two orbits are the rank 3 and the 2-transitive actions described above. Details of these constructions can be found in Conway (1969) and (1971), Conway and Sloane (1988), and Thompson (1983).

7.8 Notes

- Exercises 7.1.3–6: Homeo($\mathbb{Q}$) has been extensively studied. See, for example, Neumann (1985b), Mekler (1986) and Mekler et al.(1993).
- Lemma 7.1A: This is classical. See Wielandt (1964).

- Exercises 7.1.7–7.1.11: See Alperin (1965).
- Theorems 7.2A and 7.2B: Versions of these theorems were known to Jordan. See Wielandt and Huppert (1958) and Wielandt (1974).
- Exercises 7.2.5–7.2.8: See Wielandt (1964) Sect. 12.
- Theorems 7.2C and 7.2D: See Cameron (1981b).
- Sect. 7.2: The proof of Theorem 4.1B given here is from Burnside (1911).
- Theorem 7.2F: See Aschbacher (1972).
- Theorem 7.3A: See Wielandt (1960a). The improved result due to Nagao and Suzuki appears in Huppert and Blackburn (1982) §XII.4.
- Sect. 7.4: Much of this section is classical, at least in the finite case. Our presentation uses Neumann (1985a); the latter also includes some of the history of the development of these results. Prior to the classification of finite simple groups, Hall (1962) and Kantor (1969) and (1974) classified some particular classes of finite Jordan groups. Using the classification of finite simple groups, S.A. Adeleke and P.M. Neumann classify infinite Jordan groups which are not highly transitive [see Neumann (1985a)]. See also Cameron (1990) and Liebeck (1983).
- Exercise 7.4.11: See Levingston and Taylor (1976).
- Exercises 7.4.12–13: See Williamson (1973).
- Lemma 7.4D and Theorem 7.4D: See Neumann (1975b). See also Levingston (1978).
- Theorem 7.5A: Often ascribed to Witt, but appears in this form in Manning (1921).
- Exercises 7.5.3–6: See Witt (1938a). See also Biggs and White (1979) and Rotman (1995).
- Theorem 7.5B: See Zassenhaus (1935).
- Sect. 7.6: Further details about the finite case may be found in Passman (1968) and Huppert and Blackburn (1982). For the infinite case see Kerby (1974) and Gründhofer (1989).
- Exercises 7.6.3–5: See B.H. Neumann (1940).
- Examples 7.6.3–5: See Karzel (1965) or Kerby (1974).
- Sect. 7.7: The following are relevant: Cameron (1972) and (1981a), Curtis et al. (1976), G. Higman (1969), Huppert (1957), Mortimer (1980), Ree (1964) and Wielandt (1967a).

8

The Structure of the Symmetric Groups

The present chapter studies the symmetric groups with particular emphasis on the infinite case. Of course we know that every group is isomorphic to a subgroup of some symmetric group (for example, via its regular permutation representation), so one might suppose that it is not possible to say much useful about the symmetric groups unless we know a great deal about groups in general. However this is not true. There are certain facts which are available without a detailed knowledge of all of the subgroups, much in the same way that we have useful results about the set of real numbers without knowing detailed facts about individual real numbers.

This chapter starts with the complete description of all normal subgroups of $Sym(\Omega)$, and then shows that (with notable exception of degree 6) the automorphisms of $Sym(\Omega)$ are all inner. We then look at the subgroups of the "small" subgroup $FSym(\Omega)$, and (at the other extreme) the subgroups of small index in $Sym(\Omega)$ and maximal subgroups of the symmetric group. Since we shall be especially interested in the case where Ω is infinite, this chapter requires a little more familiarity with set theoretic arguments and elementary results in cardinal arithmetic than previous chapters.

8.1 The Normal Structure of $Sym(\Omega)$

In Sect. 3.3 we showed that, when Ω is finite and $|\Omega| \geq 5$, then the only normal subgroups of $Sym(\Omega)$ are 1, $Alt(\Omega)$ and $Sym(\Omega)$. In the present section we are going to look at the normal subgroups of $Sym(\Omega)$ when Ω is infinite. In this case we already know of one other normal subgroup, namely the finitary symmetric groups $FSym(\Omega)$, consisting of all elements of $Sym(\Omega)$ with finite support. There is a natural generalization of this construction as follows.

Let $\mathbf{c}$ be an infinite cardinal. Then for any nonempty set Ω we define

$$Sym(\Omega, \mathbf{c}) := \{x \in Sym(\Omega) \mid |\mathrm{supp}(x)| < \mathbf{c}\}.$$

Exercise

8.1.1 Show that $Sym(\Omega, \mathbf{c})$ is a normal subgroup of $Sym(\Omega)$ for every infinite cardinal $\mathbf{c}$. When $\mathbf{c} = \aleph_0$ (the smallest infinite cardinal), then $Sym(\Omega, \aleph_0) = FSym(\Omega)$, and $Sym(\Omega, \mathbf{c}) = Sym(\Omega)$ whenever $\mathbf{c} > |\Omega|$.

The primary object of this section is to prove the following theorem which shows that the only normal subgroups of $Sym(\Omega)$ are the obvious ones. The result is due to Baer (1934).

Theorem 8.1A. *Let Ω be any set with $|\Omega| > 4$. Then the normal subgroups of $Sym(\Omega)$ are precisely: 1, $Alt(\Omega)$, $Sym(\Omega)$ and the subgroups of the form $Sym(\Omega, \mathbf{c})$ with $\aleph_0 \leq \mathbf{c} \leq |\Omega|$.*

Exercises

8.1.2 Find all normal subgroups of S_n for $n = 1, 2, 3$ and 4. [*Hint:* In the respective cases there are 1, 2, 3 and 4 normal subgroups.]

8.1.3 Show that $Sym(\Omega, \mathbf{c})$ has order $|\Omega|$ for $\mathbf{c} = \aleph_0$ and order $|\Omega|^{\mathbf{c}}$ for $\aleph_0 < \mathbf{c} \leq |\Omega|$.

8.1.4 If G is an infinite subgroup of $FSym(\Omega)$, show that for each $\alpha \in \Omega$ we have $|G_\alpha| = |G|$.

The proof of Theorem 8.1A is based on three lemmas.

Lemma 8.1A. *For each $x \in Sym(\Omega)$ there exist $y, z \in Sym(\Omega)$ such that $x = yz$, $y^2 = z^2 = 1$ and $\operatorname{supp}(y) \cup \operatorname{supp}(z) \subseteq \operatorname{supp}(x)$.*

Proof. It is enough to prove the result for each of the disjoint cycles of x. In the case of a finite cycle we may consider, without loss in generality, a cycle of the form $(1\ 2 \dots n)$. Define

$$y := (1\ 2m)(2\ 2m-1)\dots(m\ m+1),$$
$$z := (2\ 2m)(3\ 2m-1)\dots(m\ m+2), \text{ and}$$
$$w := (1\ 2m+1)(2\ 2m)\dots(m\ m+2).$$

Then $yz = (1\ 2 \dots 2m)$ and $yw = (1\ 2 \dots 2m+1)$, so the case of a finite cycle is settled. On the other hand an infinite cycle $(\dots -1\ 0\ 1\ 2 \dots)$ can be written as the product yz where:

$$y := (0\ 1)(-1\ 2)(-2\ 3)\dots, \text{ and}$$
$$z := (0\ 2)(-1\ 3)(-2\ 4)\dots$$

This proves the lemma. □

Lemma 8.1B. *Let $N \lhd Sym(\Omega)$ and suppose that some $x \in N$ has $|\operatorname{supp}(x)| = \mathbf{a} \geq \aleph_0$. Then for each infinite cardinal $\mathbf{b} \leq \mathbf{a}$ there exists $y \in N$ of order 2 with $\mathbf{b}$ 2-cycles and at least $\mathbf{b}$ fixed points.*

PROOF. We first define an element $z \in Sym(\Omega)$ with the same cycle structure as x (so z is conjugate to x in $Sym(\Omega)$), such that $\mathrm{supp}(z) = \mathrm{supp}(x)$, and xz has exactly $\mathbf{b}$ 2-cycles (and perhaps nontrivial cycles of other lengths). We do this as follows:

(i) For each finite cycle $u = (\alpha_1\alpha_2 \dots \alpha_n)$ of length ≥ 4 in x there will be a corresponding cycle $v = (\alpha_4\alpha_1\alpha_2\alpha_3 \dots)$ in z with the same support. Note that uv contains the 2-cycle $(\alpha_1\alpha_3)$.

(ii) For each infinite cycle $u = (\dots\alpha_{-1}\alpha_0\alpha_1\dots)$ in x there will be a corresponding infinite cycle v in z with the same support where each block $\alpha_{4i}\alpha_{4i+1}\alpha_{4i+2}\alpha_{4i+3}$ in u has been replaced by the block $\alpha_{4i+3}\alpha_{4i+1}\alpha_{41+2}\alpha_{4i}$. The product uv has infinitely many 2-cycles of the form $(\alpha_{4i}\alpha_{4i+2})$.

(ii) Partition the 2-cycles of x into pairs; if there is an odd one left over then z will include that 2-cycle. For each pair $u = (\alpha_1\alpha_2)(\alpha_3\alpha_4)$ of 2-cycles in x, there will be a pair $v = (\alpha_1\alpha_3)(\alpha_2\alpha_4)$ of 2-cycles in z. Note that uv is a product of two 2-cycles.

(iv) Finally, partition the 3-cycles of x into pairs; if there is an odd one left over then z will include that 3-cycle. For each pair $u = (\alpha_1\alpha_2\alpha_3)(\alpha_4\alpha_5\alpha_6)$ of 3-cycles in x, there will be a pair $v = (\alpha_1\alpha_3\alpha_5)(\alpha_2\alpha_4\alpha_6)$ of 3-cycles in z. Note that uv is again a product of two 2-cycles.

It is now evident that z has the properties claimed. Since z is conjugate to x in $Sym(\Omega)$, $z \in N$, and so $w := xz \in N$ is an element with exactly $\mathbf{b}$ 2-cycles (and perhaps other nontrivial cycles).

Finally, form $\mathbf{b}$ pairs of 2-cycles from the 2-cycles in w leaving $\mathbf{b}$ 2-cycles unpaired. Define $t \in Sym(\Omega)$ to be a permutation with the same cycle structure as w (and so t also lies in N) in the following way. For each of the pairs $u = (\alpha_1\alpha_2)(\alpha_3\alpha_4)$ of 2-cycles in w, t has the pair $v = (\alpha_1\alpha_3)(\alpha_2\alpha_4)$ of 2-cycles; and for every other cycle r in w there is the cycle r^{-1} in t. Then $y := wt$ has precisely $\mathbf{b}$ 2-cycles and its other cycles all have length 1. □

Lemma 8.1C. *Let N be a nontrivial normal subgroup of $Sym(\Omega)$ where $|\Omega| > 4$. Then either $N = Alt(\Omega)$ or $N \geq Sym(\Omega, \aleph_0)$.*

PROOF. First recall that any nontrivial normal subgroup of the highly transitive group $S := Sym(\Omega, \aleph_0)$ is also highly transitive and hence primitive (Corollary 7.2A). Thus Theorem 3.3A shows that either $S \cap N = 1$ or $S \cap N \geq Alt(\Omega)$. We must show that the former is impossible, and that in the latter case either $N = Alt(\Omega)$ or $N \geq S$.

First suppose that $N \leq S$. Then $S \cap N = N \neq 1$ and so $N \geq Alt(\Omega)$. Since $|S : Alt(\Omega)| = 2$, this shows that $N = Alt(\Omega)$ or S as required. On the other hand, if N is not contained in S, then N contains an element of infinite support. Thus by Lemma 8.1B there exists $y \in N$ such that y has $\aleph_0$ 2-cycles and infinitely many fixed points. Let α and β be distinct fixed points of y. Then y and $z := y(\alpha\beta)$ have the same number of 2-cycles

and the same number of fixed points, and so are conjugate in $Sym(\Omega)$ (Exercise 1.2.7). Thus $z \in N$ and so $(\alpha\beta) = y^{-1}z \in N$. Therefore $N \geq \langle Alt(\Omega), (\alpha\beta)\rangle = S$ in this case. □

PROOF OF THEOREM 8.1A. Let $N \triangleleft Sym(\Omega)$ and suppose that $N \neq 1$ or $Alt(\Omega)$. Then Lemma 8.1C shows that $N \geq Sym(\Omega, \aleph_0)$. Let $\mathbf{b}$ be the least cardinal such that $|\text{supp}(x)| < \mathbf{b}$ for all $x \in N$. Then $N \leq Sym(\Omega, \mathbf{b})$ and we want to show that $N = Sym(\Omega, \mathbf{b})$. By Lemma 8.1A it is enough to show that each element $y \in Sym(\Omega, \mathbf{b})$ with order 2 lies in N, and since $N \geq Sym(\Omega, \aleph_0)$ it is enough to do this when $\mathbf{a} := |\text{supp}(y)| \geq \aleph_0$. Since $\mathbf{a} < \mathbf{b}$, the definition of $\mathbf{b}$ shows that there exists $x \in N$ with $\mathbf{c} := |\text{supp}(x)| \geq \mathbf{a}$, and then Lemma 8.1B shows that there exists $z \in N$ of order 2 with $\mathbf{a}$ 2-cycles and $|\Omega|$ 1-cycles. This means that z is conjugate to y in $Sym(\Omega)$ provided they have the same number of fixed points (= 1-cycles). Since $|\Omega| \geq \mathbf{a}$, the only case in which the numbers of fixed points can differ is when $\mathbf{a} = |\Omega|$ and $|\text{fix}(y)| < |\text{fix}(z)| = \mathbf{a}$. In this case there is a permutation $t \in Sym(\Omega)$ which maps $\text{supp}(z)$ into $\text{supp}(y)$ in such a way that 2-cycles are mapped onto 2-cycles. Then all the 2-cycles in $t^{-1}zt$ appear as 2-cycles in y, but there are $\mathbf{a}$ 2-cycles in y which do not appear as 2-cycles in $t^{-1}zt$ (the support of the latter cycles lies in $\text{fix}(z)^t$). Hence $w := yt^{-1}zt$ has exactly $\mathbf{a}$ 2-cycles and $\mathbf{a}$ 1-cycles which means that w (and hence y) is conjugate to an element in N. Thus in either case y is conjugate to an element in N. Since $N \triangleleft Sym(\Omega)$, this implies $y \in N$ as required. This proves the theorem. □

Exercises

8.1.5 Let $\mathbf{c}$ be an infinite cardinal. Show that two elements $x, y \in Sym(\Omega, \mathbf{c})$ are conjugate in $Sym(\Omega)$ if and only if they are conjugate in $Sym(\Omega, \mathbf{c})$. Deduce that every normal subgroup of $Sym(\Omega, \mathbf{c})$ is normal in $Sym(\Omega)$.

8.1.6 Let $\mathbf{a}$ be an arbitrary infinite cardinal, and let $\mathbf{b}$ be the least cardinal with $\mathbf{a} < \mathbf{b}$. Show that for any set Ω with $|\Omega| > \mathbf{a}$, $Sym(\Omega, \mathbf{b})/Sym(\Omega, \mathbf{a})$ is a simple group.

8.1.7 Show that any nontrivial factor group $Sym(\Omega, \mathbf{a})/Sym(\Omega, \mathbf{b})$ has elements of infinite order.

8.1.8 Prove that no two distinct normal subgroups of $Sym(\Omega)$ are isomorphic. Moreover, if $M \triangleleft Sym(\Omega)$ and $N \triangleleft Sym(\Lambda)$ with $M \cong N \neq 1$, then $|\Omega| = |\Lambda|$.

8.1.9 Show that every group is isomorphic to a subgroup of some simple group.

8.1.10 Find necessary and sufficient conditions on the cycle lengths of two permutations in $Sym(\Omega)$ in order that they should be conjugate under an element of $Alt(\Omega)$. In particular, show that each conjugacy class of $FSym(\Omega)$ contained in $Alt(\Omega)$ is either a conjugacy class of $Alt(\Omega)$, or a union of two conjugacy classes.

8.2 The Automorphisms of $Sym(\Omega)$

Theorem 8.1A shows that $Sym(\Omega)$ has a rather rigid normal structure with a single chain of normal subgroups, so it is not too surprising that the automorphisms of $Sym(\Omega)$ are quite tightly controlled as well. As we shall see below, except for the notable exception when $|\Omega| = 6$, the automorphisms of $Sym(\Omega)$ are all inner. In the infinite case, these theorems are due to Schreier and Ulam (1936). We begin with a slightly more general result.

Theorem 8.2A. *Let $|\Omega| > 6$. Suppose that G satisfies $Alt(\Omega) \leq G \leq Sym(\Omega)$, and let N be the normalizer of G in $Sym(\Omega)$. Then for each automorphism ϕ of G there exists $y \in N$ such that $x^\phi = y^{-1}xy$ for all $x \in G$. In particular, every automorphism of $Sym(\Omega)$ is inner.*

The theorem remains true for $|\Omega| < 6$, but is false for $|\Omega| = 6$. (See Exercises 8.2.2–8.2.5.) The proof of the theorem will be based on two lemmas.

Lemma 8.2A. *Under the hypotheses of the theorem, ϕ maps $Alt(\Omega)$ onto itself and so its restriction to $Alt(\Omega)$ is an automorphism of $Alt(\Omega)$. Moreover, if C is the conjugacy class consisting of all 3-cycles in $Alt(\Omega)$ then $C^\phi = C$.*

PROOF. Put $A := Alt(\Omega)$. Since $|\Omega| > 4$, A is simple and the same is true of A^ϕ. Since A and A^ϕ are both normal in G, $A \cap A^\phi$ is normal in both A and A^ϕ, and so either $A \cap A^\phi = 1$ or $A = A^\phi$. The former case could only happen if A^ϕ centralized A. Since the centralizer of A in $Sym(\Omega)$ is trivial (see Exercise 8.2.1), we conclude that $A = A^\phi$, and so the restriction of ϕ to A is an automorphism of A. It remains to show that $C = C^\phi$.

We begin with a characterization: C is the unique conjugacy class of A consisting of elements of order 3 such that for all $x, y \in C$, xy has order 1, 2, 3 or 5. (The latter fact follows from the calculations $(123)(145) = (12345)$, $(123)(124) = (14)(23)$ and $(123)(214) = (234)$.) Since it is easy to see that C^ϕ is also a conjugacy class of A, it is enough to show that C is the only conjugacy class with these properties. Let C' be another conjugacy class of A consisting of elements of order 3 with $C' \neq C$. Then each element in C' contains at least two 3-cycles. Since $|\Omega| \geq 7$ by hypothesis, the calculation

$$(137)(254)\dots(253)(467)\dots = (123456\dots)\dots$$

shows that there are two elements $x, y \in C'$ such that xy has order at least 6. Thus $C^\phi \neq C'$, and the lemma is proved. □

Lemma 8.2B. *Under the hypotheses of the theorem, if ψ is an automorphism of G which fixes each element of $Alt(\Omega)$, then ψ is the identity map.*

PROOF. Let $y \in G$. Then for each $x \in Alt(\Omega)$, we have $y^{-1}xy \in Alt(\Omega)$ and so $y^{-1}xy = (y^{-1}xy)^\psi = (y^\psi)^{-1}xy^\psi$. Thus $y^\psi y^{-1}$ centralizes $Alt(\Omega)$. Since $|\Omega| > 3$, the centralizer of $Alt(\Omega)$ is trivial, and so $y^\psi = y$ for all $y \in G$. □

PROOF OF THEOREM 8.2A. For each pair of distinct points $\alpha, \beta \in \Omega$ define

$$L(\alpha, \beta) := \{(\alpha\beta\gamma) \in C \mid \gamma \in \Omega \setminus \{\alpha, \beta\}\}.$$

Then the calculations in the proof of Lemma 8.2A show that $S := L(\alpha, \beta)$ is maximal as a subset of C satisfying the condition

(8.1) if $x, y \in S$ and $x \neq y$, then xy has order 2.

The same calculations show that, conversely, if S is a subset of C which satisfies (8.1) and contains $(\alpha\beta\gamma)$, then S is a subset of $L(\alpha, \beta), L(\beta, \gamma)$ or $L(\gamma, \alpha)$. Thus $L(\alpha, \beta)$ ($\alpha, \beta \in \Omega$ and $\alpha \neq \beta$) are the unique maximal subsets of C with the property (8.1). Since the property (8.1) is invariant under automorphisms of $Alt(\Omega)$, Lemma 8.2A shows that the sets $L(\alpha, \beta)$ are permuted amongst themselves by ϕ. In particular, if we fix α and β with $\alpha \neq \beta$, then there exist α' and β' with $\alpha' \neq \beta'$ such that $L(\alpha, \beta)^\phi = L(\alpha', \beta')$.

Now define $y \in Sym(\Omega)$ by: $\alpha^y = \alpha', \beta^y = \beta'$, and $\gamma^y = \gamma'$ such that $(\alpha\beta\gamma)^\phi = (\alpha'\beta'\gamma')$ for all $\gamma \neq \alpha$ or β. Let ψ be the homomorphism of G into $Sym(\Omega)$ defined by $x^\psi := yx^\phi y^{-1}$. Then, for all $\gamma \neq \alpha$ or β we have $(\alpha\beta\gamma)^\psi = (\alpha\beta\gamma)$, so ψ fixes each element of $L(\alpha, \beta)$. Since $L(\alpha, \beta)$ generates $Alt(\Omega)$ (see Exercise 1.6.8), we conclude that ψ acts trivially on $Alt(\Omega)$ and so ψ is the identity on G by Lemma 8.2B. Thus $x^\phi = y^{-1}xy$ for all $x \in G$. In particular, this shows that $y \in N$, and the theorem is proved. □

Exercises

8.2.1 Show that the centralizer of $Alt(\Omega)$ in $Sym(\Omega)$ is trivial if $|\Omega| > 3$.

8.2.2 Show that Theorem 8.2A remains true when $|\Omega| < 6$. [*Hint:* For $|\Omega| = 4$ or 5, show that the conclusions of the two lemmas remain true.]

8.2.3 Show that $\langle(12345), (2354)\rangle$ is a subgroup of index 6 in S_5, and hence that S_5 has a faithful transitive permutation representation of degree 6 in which each element of order 3 is fixed point free.

8.2.4 From Exercise 8.2.3 it follows that S_6 has two conjugacy classes of subgroups isomorphic to S_5: a class of transitive subgroups and a class of intransitive subgroups. Show that there is an automorphism of S_6 which interchanges these two classes (and hence cannot be an inner automorphism).

8.2.5 Show that $\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6)$ has order 2.

8.3 Subgroups of $FSym(\Omega)$

The present section considers some of the properties of the finitary symmetric group $FSym(\Omega)$ when Ω is infinite. We begin with the following crucial observation. Theorem 3.3D shows that every primitive subgroup of $Sym(\Omega)$ which contains a nontrivial element of finite support must contain all of $Alt(\Omega)$. Since $|FSym(\Omega) : Alt(\Omega)| = 2$, we obtain the following lemma.

Lemma 8.3A. *If Ω is infinite, $Alt(\Omega)$ and $FSym(\Omega)$ are the only primitive subgroups of $FSym(\Omega)$.*

Consider now an imprimitive subgroup G of $FSym(\Omega)$. If Δ is proper block for G, then there exists $x \in G$ such that $\Delta \cap \Delta^x = \emptyset$, and so $\Delta \subseteq \mathrm{supp}(x)$. Since the latter is finite, this shows that each proper block of G is finite. There are then two cases which may arise:

(i) G has a maximal proper block Δ (so Ω is the only other block containing Δ);
(ii) G has no maximal proper block and so there exists an infinite strictly ascending sequence of finite blocks

$$\Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_k \subset \ldots . \tag{8.2}$$

In case (i) we shall say that G is *almost primitive* and in case (ii) we shall say that G is *totally imprimitive.* This terminology comes from P. M. Neumann (1975a).

Lemma 8.3B. *Let Ω be an infinite set, and let G be a subgroup of $FSym(\Omega)$.*

(i) *Suppose that G is almost primitive, and Δ is a maximal proper block for G. Let $\Sigma := \{\Delta^x \mid x \in G\}$ be the corresponding system of blocks for G. Then the image of the action of G on Σ is either $Alt(\Sigma)$ or $FSym(\Sigma)$. (Note that $|\Sigma| = |\Omega|$ because $|\Delta|$ is finite.)*
(ii) *If G is totally imprimitive with a strictly ascending sequence (8.2) of blocks, then Ω is a countable set and $G = \bigcup G_k$ where $G_k \lhd G$ is the subgroup which fixes setwise each of the blocks Δ_k^u $(u \in G)$.*
(iii) *If G is transitive, then G has a normal subgroup K in which each simple section is finite and such that $G/K \cong 1$, $Alt(\Omega)$ or $FSym(\Omega)$.*

PROOF. (i) G acts transitively on Σ and, if Γ is a block for G on Σ with $\Delta \in \Gamma$, then the union of the blocks in Γ forms a block for G on Ω containing Δ. By the maximality of Δ, this means that G acts primitively on Σ. Because $G \leq FSym(\Omega)$, the image of the action on Σ lies in $FSym(\Sigma)$, and so the result follows from Lemma 8.3A.

(ii) Since $\bigcup \Delta_k$ is a block for G and is not finite, therefore $\Omega = \bigcup \Delta_k$. Since the Δ_k are all finite, this shows that Ω is countable. Moreover, each

$x \in G$ has finite support, therefore $\mathrm{supp}(x) \subseteq \Delta_k$ for some k. Since Δ_k is a block, this implies that, for each $u \in G$, either $\mathrm{supp}(x) \subseteq \Delta_k^u$ or $\mathrm{supp}(x) \cap \Delta_k^u = \emptyset$; hence $x \in G_k$. This proves (ii).

(iii) If G is primitive, take $K = 1$. If G is almost primitive, then let K be the kernel of the action of G on Σ defined above and note that $FSym(\Sigma) \cong FSym(\Omega)$. If G is totally imprimitive, take $K = G$. □

Lemma 8.3C. *Let $H \lhd G \leq FSym(\Omega)$ for an infinite set Ω.*

(i) *If all orbits of H are infinite, then $G' \leq H$.*

(ii) *If G is transitive, then G' is contained in every subgroup of finite index in G and the centre $Z(G)$ of G equals 1.*

PROOF. (i) Let $x, y \in G$ and put $\Delta := \mathrm{supp}(x) \cup \mathrm{supp}(y)$. Since Δ is finite and each orbit of H is infinite, Lemma 3.3B shows that there exists $u \in H$ such that $\Delta \cap \Delta^u = \emptyset$. Put $w := [x, u][y, u][(xy)^{-1}, u]$. Since $H \lhd G$ we have $w \in H$. The elements $u^{-1}xu, u^{-1}yu$ and $u^{-1}xyu$ all have supports lying in Δ^u, so they commute with both x and y. Hence

$$w = (x^{-1}y^{-1}xy)(u^{-1}xu)(u^{-1}yu)(u^{-1}y^{-1}x^{-1}u) = [x, y].$$

Thus $[x, y] \in H$ for all $x, y \in G$, and so $G' \leq H$.

(ii) If $H \leq G$ has finite index, then Exercise 1.3.4 shows that there is a normal subgroup K of finite index in G such that $K \leq H$. Then Theorem 1.6A shows that each orbit of K is infinite because G is transitive of infinite degree; hence (i) shows that $G' \leq K \leq H$. Finally, if $z \in Z(G)$, then $\mathrm{supp}(z)$ is a finite G-invariant subset of Ω, and so by the transitivity of G, $\mathrm{supp}(z) = \emptyset$ and $z = 1$. This shows that $Z(G) = 1$. □

A group G is called an *FC-group* if each conjugacy class of elements is finite (or, equivalently, if $|G : C_G(x)|$ is finite for each $x \in G$). A group G is *residually finite* if for each nontrivial element x there is a homomorphism ϕ of G onto a finite group with $\phi(x) \neq 1$. Since any subgroup of finite index in G contains a subgroup of finite index which is normal in G (see Exercise 1.3.4), G is residually finite exactly when for each $x \neq 1$ in G there is a subgroup K of finite index in G such that $x \notin K$.

Lemma 8.3D. *Let $G \leq FSym(\Omega)$. Then the following are equivalent:*

(i) *Every orbit of G is finite;*

(ii) *G is an FC-group;*

(iii) *G is residually finite.*

PROOF. (i) ⇒ (ii) Suppose that each orbit of G is finite. Then, for each $x \in G$ there is a finite G-invariant subset Δ such that $\mathrm{supp}(x) \subseteq \Delta$. The number of conjugates of x in G is then clearly bounded by the number of conjugates of x^Δ in $Sym(\Delta)$. This shows that G is an FC-group.

(ii) ⇒ (iii) Suppose that G is an FC-group. Let $x \neq 1$ be an element of G. If $x \notin Z(G)$, then there exists $y \in G$ with $x \notin C_G(y)$, and $C_G(y)$ has

finite index by (ii). On the other hand, if $x \in Z(G)$, then $\Delta := \text{supp}(x)$ is a finite G-invariant set, and so $G_{(\Delta)}$is a subgroup of finite index in G not containing x. This shows that G is residually finite.

(iii) $\Rightarrow$ (i) Suppose that G is residually finite, and let Γ be an orbit for G. If Γ is infinite, then $G^{\Gamma}$is also residually finite and so Lemma 8.3C (ii) shows that $(G^{\Gamma})' = 1$. But then $Z(G^{\Gamma}) = G^{\Gamma}$ contrary to Lemma 8.3C (ii). Hence the orbits for G must all be finite. This completes the proof. □

Exercises

8.3.1 Define the subsets $T_k (k = 1, 2, \ldots.)$ of $FSym(\mathbb{N})$ by

$$T_1 := \{(01), (23), (45), \ldots\}$$
$$T_2 := \{(02)(13), (46)(57), \ldots\}$$
$$\vdots$$

where in general T_k consists of all elements of the form

$$x_{k,n} := \prod_{i=0}^{2^{k-1}-1} (i + n2^k, i + n2^k + 2^{k-1}).$$

for $n = 0, 1, \ldots.$ Let G be the union of the subgroups $G_k := \langle T_1, \ldots, T_k \rangle$ for $k = 1, 2, \ldots.$ Show that:

(i) for each k, $G_k \lhd G$, and G_{k+1}/G_k is an elementary abelian 2-group;

(ii) all finitely generated subgroups of G are finite 2-groups;

(iii) G is transitive.

8.3.2 Let p be a prime, and define G to be the multiplicative group consisting of all complex numbers z such that $z^{p^k} = 1$ for some $k \geq 1$. Show that G has no nontrivial representation as a finitary permutation group.

8.3.3 Suppose that $H \lhd N \lhd G \leq FSym(\Omega)$ for some infinite set Ω. If all orbits of N are infinite, show that $H \lhd G$.

We now consider the class $\mathcal{X}$ of groups G with the property that every (not necessarily faithful) representation of G as a group of finitary permutations has all of its orbits finite. Every finite group lies in $\mathcal{X}$. If $G \in \mathcal{X}$, then each factor group $G/N \in \mathcal{X}$. Since the class of FC-groups is clearly closed under taking factor groups, it follows from Lemma 8.3D that every FC-group lies in $\mathcal{X}$. In general, $G \in \mathcal{X}$ does not imply that each subgroup $H \in \mathcal{X}$. Indeed, $Sym(\mathbb{N}) \in \mathcal{X}$ (see Exercise 8.3.4 below), but $FSym(\mathbb{N}) \notin \mathcal{X}$.

Exercise

8.3.4 Show that $Sym(\mathbb{N}) \in \mathcal{X}$. [*Hint:* Use Theorem 8.1A and Lemma 8.3B.]

As noted above, $\mathcal{X}$ is not closed under taking subgroups, but, as the next lemma shows, $\mathcal{X}$ is closed under forming extensions.

Lemma 8.3E.
(i) *If $H \lhd G \leq FSym(\Omega)$ with $H \neq 1$ and $G/H \in \mathcal{X}$, then H is transitive on every infinite orbit of G.*
(ii) *If $N \lhd K$ and both N and K/N lie in $\mathcal{X}$, then $K \in \mathcal{X}$.*

PROOF. (i) It is enough to consider the case where Ω is infinite and G is transitive; we have to show that H is also transitive. Suppose the contrary. Then G is imprimitive and the set Σ of orbits of H form a system of nontrivial blocks for G. Since all proper blocks for G are finite by Lemma 8.3B, Σ is infinite. Consider the action of G on Σ. This action gives a homomorphism of G onto a transitive subgroup of $FSym(\Sigma)$ with a kernel K. Thus $G/K \notin \mathcal{X}$. Clearly $H \leq K$, and therefore G/H cannot lie in $\mathcal{X}$. This contradicts the hypothesis on H. Hence H must be transitive.

(ii) Let $\sigma : K \to FSym(\Omega)$ be any representation as a group of finitary permutations. Since $\sigma(K)/\sigma(N)$ is a homomorphic image of K/N we have $\sigma(K)/\sigma(N) \in \mathcal{X}$. Therefore applying (i) to $\sigma(N) \lhd \sigma(K) \leq FSym(\Omega)$ we see that $\sigma(N)$ is transitive on every infinite orbit of $\sigma(K)$. Since $N \in \mathcal{X}$, this implies that $\sigma(K)$ has no infinite orbits. Since this is true for every finitary representation σ of K, we have $K \in \mathcal{X}$. □

The next theorem gives examples of further classes of groups in $\mathcal{X}$. A group G has *finite exponent* if for some integer $m \geq 1$ we have $x^m = 1$ for all $x \in$ G. A group G is *hypercentral* if every factor group $G/N \neq 1$ has a nontrivial centre $Z(G/N)$. A finite group is hypercentral exactly when it is nilpotent, but infinite hypercentral groups can be much more complicated [see, for example, Robinson (1972)].

Theorem 8.3A. *All groups in the following classes lie in $\mathcal{X}$:*
(i) *groups of finite exponent;*
(ii) *hypercentral groups;*
(iii) *solvable groups.*

PROOF. (i) Since the class of groups of finite exponent is closed under taking homomorphic images, it is enough to show that if $G \leq FSym(\Omega)$ is an infinite transitive group, then G contains elements of arbitrarily large orders. This is true if G is almost primitive by Lemma 8.3B since the infinite alternating group contains elements of arbitrarily large order. Thus it remains to consider the totally imprimitive case.

We shall proceed by induction on n to show that every infinite, transitive, totally imprimitive group $G \leq FSym(\Omega)$ has an element with a cycle of length $> n$. This is clearly true for $n = 1$, so suppose that $n > 1$. Choose $x \neq 1$ in G. Then G has a finite block Δ such that $\mathrm{supp}(x) \subseteq \Delta$ (Lemma 8.3B). Let Σ be the system of blocks Δ^x $(x \in G)$. Since Δ is finite, Σ

is infinite, and G acts as a totally imprimitive group on Σ. Hence by the induction hypothesis, there exists $y \in G$ whose action on Σ contains a cycle of length $h \geq n$. Since G is transitive on Σ we may choose y so that $\Delta, \Delta^y, \ldots, \Delta^{y^{n-1}}$ are all distinct. If $\alpha \in \text{supp}(x) \subseteq \Delta$, then an easy induction on i shows that

$$\alpha^{(xy)^i} = (\alpha^x)^{y^i} \in \Delta^{y^i} \quad \text{for } i = 1, 2, \ldots, n-1.$$

In particular, the cycles in xy and y which contain α have length at least n. However, at least one of these cycles must have length greater than n, since otherwise from above we have

$$\alpha = \alpha^{(xy)^{n-1}} = (\alpha^x)^{y^{n-1}} = \alpha^x$$

which contradicts the choice of $\alpha \in \text{supp}(x)$. This proves the induction step and so the result is proved.

(ii) Again, since the class of hypercentral groups is closed under taking homomorphic images, it is enough to show that if $G \leq FSym(\Omega)$ is a transitive, hypercentral group, then Ω is finite. But this follows from Lemma 8.3C (ii) because a nontrivial hypercentral group has a nontrivial centre.

(iii) Since abelian groups are hypercentral, (ii) and Lemma 8.3E show that every solvable group lies in $\mathcal{X}$. □

Corollary 8.3A. *Let $G \leq FSym(\Omega)$ be an infinite transitive group. Then G' is the unique minimal normal transitive subgroup of G. In particular, $G' = G''$ (so G' is perfect).*

PROOF. Lemma 8.3D shows that every transitive normal subgroup contains G'. Since $G/G' \in \mathcal{X}$ by the theorem, G' is transitive by Lemma 8.3E. It now follows that $G''(= (G')')$ is also transitive. Since G'' is a normal subgroup of G which is contained in G', therefore $G'' = G'$. □

Exercise

8.3.5 We say that a group G is *residually-$\mathcal{X}$* if for each nontrivial $x \in G$ there exists $K \lhd G$ such that $x \notin K$ and $G/K \in \mathcal{X}$. If $G \leq FSym(\Omega)$ and G is residually$-\mathcal{X}$, show that all orbits of G are finite, and hence that G is residually finite.

8.4 Subgroups of Small Index in $Sym(\Omega)$

We have seen in Sect. 5.2 that a subgroup of "small index" in S_n, namely, of index less than $\frac{1}{2}\binom{n}{\lfloor n/2 \rfloor}$, either contains A_n or is intransitive (with a few exceptions for small n). In the theorem below we consider the analogous theorem in the case where the symmetric group has countably infinite degree. The case where the degree is uncountable is also interesting although

we shall not consider it here; the analogous results are dependent on the validity of the "Generalized Continuum Hypothesis".

Theorem 8.4A. *Let Ω be countably infinite and put $S := Sym(\Omega)$. Then for any subgroup G of S the following conditions are equivalent:*
(i) $|S : G| < 2^{|\Omega|}$;
(ii) *for some finite subset* $\Delta \subseteq \Omega$, $S_{(\Delta)} \leq G \leq S_{\{\Delta\}}$;
(iii) $S = FSym(\Omega)G$.

The proof of the theorem will be based on two lemmas. In the arguments below we shall use the concept of a "moiety" (a term used in a legal sense for a half share): a *moiety* of an infinite set Ω is a subset Γ such that $|\Gamma| = |\Omega \setminus \Gamma|$. It is important to observe that, for any subsets $\Gamma, \Gamma' \subseteq \Omega$ with $|\Gamma| = |\Gamma'|$ and $|\Omega \setminus \Gamma| = |\Omega \setminus \Gamma'|$, there exists $x \in Sym(\Omega)$ such that $\Gamma' = \Gamma^x$; in particular, $Sym(\Omega)$ acts transitively on the set of moieties of Ω. The first lemma is a classical result of W. Sierpinski proved in 1928.

Lemma 8.4A. *Let Ω be a countable set. Then there exists a family $\mathcal{F}$ of moieties of Ω such that:*
(i) $|\mathcal{F}| = 2^{|\Omega|}$; *and*
(ii) *for any two distinct* Γ, Γ' *in* $\mathcal{F}$, $\Gamma \cap \Gamma'$ *is finite.*

Proof. Without any loss in generality we may take $\Omega = \mathbb{Q}$. Then for each real number r we choose an infinite sequence $\{\alpha_n\}$ of distinct rationals which converges to r, and define Γ_r to be the set $\{\alpha_n \mid n = 1, 2, \ldots\}$. It is now easily verified that $\mathcal{F} := \{\Gamma_r \mid r \in \mathbb{R}\}$ is a family of moieties satisfying (i) and (ii). □

As usual, if $\Sigma \subseteq \Omega$, then we identify $Sym(\Sigma)$ with the pointwise stabilizer of $\Omega \setminus \Sigma$ in $Sym(\Omega)$.

Lemma 8.4B. *Let Γ_1 and Γ_2 be subsets of an arbitrary set Ω such that $|\Gamma_1 \cap \Gamma_2| = |\Gamma_1| \leq |\Gamma_2|$. Then*

$$\langle Sym(\Gamma_1), Sym(\Gamma_2) \rangle = Sym(\Gamma_1 \cup \Gamma_2).$$

Proof. If Γ_1 is a finite set, then the hypotheses imply that $\Gamma_1 \cap \Gamma_2 = \Gamma_1$, and so the result is trivial; hence suppose that Γ_1 is infinite. Put $\Delta := \Gamma_1 \cap \Gamma_2$ and $\Sigma := \Gamma_1 \cup \Gamma_2$. Let $x \in Sym(\Sigma)$. Since $\Delta^x \subseteq \Sigma$ and Δ is infinite, there is some i such that $|\Delta^x \cap \Gamma_i| = |\Delta|$. Choose a subset Φ of Δ so that Φ^x is a moiety of $\Delta^x \cap \Gamma_i$, and note that Φ is also a moiety of Δ. Then $|\Phi| = |\Phi^x|$ and $|\Gamma_i \setminus \Phi| = |\Gamma_i| = |\Gamma_i \setminus \Phi^x|$, and so there exists $y \in Sym(\Gamma_i)$ such that $(\Gamma_i \setminus \Phi^x)^y = \Gamma_i \setminus \Phi$ and $\gamma^{xy} = \gamma$ for all $\gamma \in \Phi$. Now by the hypothesis on Δ, $|\Gamma_1 \setminus \Delta| \leq |\Delta| = |\Phi|$. Hence, for some $z \in Sym(\Gamma_1)$, we have $(\Gamma_1 \setminus \Delta)^z \subseteq \Phi$, and so $\Gamma_1 \setminus \Delta \subseteq \mathrm{fix}(zxyz^{-1})$. This shows that $zxyz^{-1} \in Sym(\Gamma_2)$, and so $x \in \langle Sym(\Gamma_1), Sym(\Gamma_2) \rangle$. Thus we

have shown that

$$\langle Sym(\Gamma_1), Sym(\Gamma_2)\rangle \geq Sym(\Gamma_1 \cup \Gamma_2).$$

The reverse inequality is trivial, so the lemma is proved. □

PROOF OF THEOREM 8.4A. Since $|FSym(\Omega)| = |\Omega| < 2^{|\Omega|}$, it is clear that (iii) implies (i). On the other hand, if Δ is a finite subset of Ω, then for each $x \in S$ there exists $y \in FSym(\Omega)$ such that $y^{-1}x \in S_{(\Delta)}$; hence $S = FSym(\Omega)S_{(\Delta)}$. This shows that (ii) implies (iii). It remains to show that (i) implies (ii).

We shall first show that there is a moiety Σ in Ω such that $Sym(\Sigma) \leq G$. Since Ω and $\Omega \times \Omega$ have the same cardinality, we can write Ω as a union of a countably infinite family $\{\Sigma_i \mid i \in \mathbb{N}\}$ of infinite subsets which are pairwise disjoint. Write $S_i := Sym(\Sigma_i)$, and define

$$T := \{x \in S \mid \Sigma_i^x = \Sigma_i \quad \text{for all } i\}.$$

Now, if $G_i \leq S_i$ denotes the restriction of $G \cap T$ to Σ_i, then $G \cap T \leq \prod_i G_i$, and so

$$\prod_i |S_i : G_i| = \prod_i |T : G_i| \leq |T : G \cap T| \leq |S : G| < 2^{|\Omega|}.$$

Since $|\Omega| = \aleph_0$, this implies that $|S_i : G_i| = 1$ for all but a finite number of values of i. If we choose j such that $S_j = G_j$ and put $\Sigma := \Sigma_j$, then $G_{\{\Sigma\}}$ acts as the full symmetric group on Σ. This implies that, whenever $u \in G \cap Sym(\Sigma)$ and $x \in Sym(\Sigma)$, then for some $v \in G$ we have $x^{-1}ux = v^{-1}uv \in G \cap Sym(\Sigma)$; hence $G \cap Sym(\Sigma) \lhd Sym(\Sigma)$. Since

$$|Sym(\Sigma) : Sym(\Sigma) \cap G| \leq |S : G| < 2^{|\Omega|}$$

and $|Sym(\Sigma) : FSym(\Sigma)| = 2^{|\Omega|}$, it follows from Theorem 8.1A that $G \cap Sym(\Sigma) = Sym(\Sigma)$. Hence $Sym(\Sigma) \leq G$ as required.

Now let $\mathcal{F}$ be a family of moieties of Σ which satisfies conditions (i) and (ii) of Lemma 8.4A. Since each $\Gamma \in \mathcal{F}$ is a moiety of Ω, we can choose an element $x(\Gamma)$ of order 2 in S such that

$$x(\Gamma) \in S_{(\Sigma \setminus \Gamma)} \quad \text{and} \quad x(\Gamma) \text{ interchanges } \Gamma \text{ and } \Omega \setminus \Sigma.$$

Since $|\mathcal{F}| > |S : G|$, there exist distinct $\Gamma, \Gamma' \in \mathcal{F}$ such that $z := x(\Gamma)x(\Gamma')^{-1} = x(\Gamma)x(\Gamma') \in G$. Put $\Sigma' := \Sigma^z$, and note that $\Sigma = \Omega \setminus (\Gamma')^{x(\Gamma')}$ and $\Sigma' = (\Omega \setminus \Gamma^{x(\Gamma)})^z = \Omega \setminus \Gamma^{x(\Gamma')}$. Hence $\Sigma \cap \Sigma' = \Omega \setminus (\Gamma \cup \Gamma')^{x(\Gamma')}$ and $\Sigma \cup \Sigma' = \Omega \setminus (\Gamma \cap \Gamma')^{x(\Gamma')}$.

In particular, $\Sigma \cap \Sigma'$ contains $(\Omega \setminus \Sigma)^{x(\Gamma')}$ because $\Gamma, \Gamma' \subseteq \Sigma$, and so $\Sigma \cap \Sigma'$ is infinite. Since $Sym(\Sigma)$ and $Sym(\Sigma') = z^{-1}Sym(\Sigma)z$ both lie in G, we conclude from Lemma 8.4B that $Sym(\Sigma \cup \Sigma') \subseteq G$. On the other hand, $\Delta' := (\Gamma \cap \Gamma')^{x(\Gamma')}$ is finite by the construction of $\mathcal{F}$, and $S_{(\Delta')} = Sym(\Sigma \cup \Sigma')$, so we conclude that $S_{(\Delta')} \subseteq G$ for the finite subset Δ'.

Finally, choose Δ to be a smallest finite subset of Ω such that $S_{(\Delta)} \subseteq G$. Then for each $x \in G$ we have $Sym(\Omega \setminus \Delta^x) = x^{-1}Sym(\Omega \setminus \Delta)x \leq G$, and so Lemma 8.4B shows that $G \geq \langle Sym(\Omega \setminus \Delta), Sym(\Omega \setminus \Delta^x)\rangle = Sym(\Omega \setminus (\Delta \cap \Delta^x))$. Thus, for all $x \in G$, $\Delta = \Delta^x$ by the minimality of Δ. Hence $G \leq S_{\{\Delta\}}$, and the proof of the theorem is complete. □

Exercises

8.4.1 Let $S := Sym(\Omega, \mathbf{c})$ where Ω is an infinite set and $\mathbf{c}$ is an infinite cardinal. Show that $S_{\{\Delta\}}$ is a maximal subgroup of S for each nonempty finite subset Δ of Ω.

8.4.2 Show that there exists a proper subgroup of $Sym(\mathbb{N})$ which acts transitively on the set of moieties of $\mathbb{N}$.

8.4.3 Show that $Sym(\mathbb{N})$ contains a free subgroup of rank $2^{\aleph_0}$.

8.5 Maximal Subgroups of the Symmetric Groups

It follows from Exercise 5.2.8 that the maximal subgroups M of S_n fall into three classes:

(i) (intransitive) M is the set stabilizer of some set of size m with $1 \leq m < n/2$, and so is isomorphic to $S_m \times S_{n-m}$;

(ii) (imprimitive) M is the stabilizer of some partition of $\{1, 2, \ldots, n\}$ into m equal parts of size k with $1 < m < n$, and so is isomorphic to the wreath product S_k *wr* S_m in its imprimitive action; or

(iii) (primitive) $M = A_n$, or else is a proper primitive group (and so has "small" order).

It is easily shown that any subgroup in class (i) or (ii) is maximal in S_n (Exercise 5.2.8), but it is much harder to decide which of the subgroups in (iii) are maximal. In Liebeck et al. (1987), the O'Nan–Scott Theorem (Theorem 4.1A) and the classification of finite simple groups are used to identify precisely which of the proper primitive subgroups of S_n are maximal in S_n (or in A_n). For example, if $n = k^m$ ($k \geq 2$, $m \geq 2$), then the subgroups of S_n which are permutation isomorphic to S_k *wr* S_m in its product action (see Lemma 4.5A) are maximal. Similarly, for any nonabelian simple group T, and $n = |T|^{m-1}$, the group $T^m \cdot (\mathrm{Out}(T) \times S_m)$ is maximal in S_n or A_n in its diagonal action (see Lemma 4.5B), and the affine group $AGL_d(p)$ is isomorphic to a primitive maximal subgroup of S_n when $n = p^d$ (p prime, $d \geq 2$).

The situation for infinite symmetric groups is more complicated, and it seems unlikely that there is any satisfactory description of the maximal subgroups in this case. The remaining theorems in this chapter give some recent results along these lines and hint at the complexity of this problem.

Exercises

8.5.1 When is $AGL_1(F)$ maximal in $Sym(F)$ (where F is a field)?
8.5.2 In general an infinite group need not have any maximal subgroup. Show that the abelian group $(\mathbb{Q}, +)$ has no maximal subgroup.
8.5.3 Let H be a subgroup of an infinite group G, and suppose that G can be generated by H and a finite set of additional elements. Show that G has at least one maximal subgroup containing H. [*Hint:* This will require a transfinite argument such as the use of Zorn's Lemma.]

We begin with some simple lemmas. In the following we shall say that a moiety Γ of Ω is *full* for some subgroup $G \leq Sym(\Omega)$ if $G_{\{\Gamma\}}$ induces the full symmetric group $Sym(\Gamma)$ in its action on Γ.

Lemma 8.5A. *Let Ω be an arbitrary infinite set, and let $G \leq S := Sym(\Omega)$. Then:*
(i) *Let Γ and Δ be moieties of Ω such that $\Sigma := \Gamma \cap \Delta$ has size $|\Omega|$ and $\Omega = \Gamma \cup \Delta$. If Γ and Δ are both full for G, then $G = S$.*
(ii) *If $G \neq S$, and at least one moiety of Ω is full for G, then there exists $x \in S$ such that $S = \langle G, x \rangle$, and so G is contained in a maximal subgroup of S.*

PROOF. (i) Since G is full on Γ, there exists $x \in G_{\{\Gamma\}}$ such that $\text{fix}_\Gamma(x) = \Gamma \setminus \Sigma = \Omega \setminus \Delta$. Then $x \in G_{(\Gamma\setminus\Sigma)} \lhd G_{\{\Gamma\setminus\Sigma\}} = G_{\{\Delta\}}$, and $|\text{supp}_\Delta(x)| = |\Delta|$ because $\text{supp}_\Delta(x) \supseteq \Sigma$ and $|\Sigma| = |\Omega|$. Now Theorem 8.1A shows that x^Δ is not contained in any proper normal subgroup of $Sym(\Delta)$. Since G is full on Δ, therefore $G_{\{\Delta\}} = G_{(\Gamma\setminus\Sigma)} = G_{(\Omega\setminus\Delta)} = Sym(\Delta)$. Hence $Sym(\Delta) \leq G$. A similar argument shows that $Sym(\Gamma) \leq G$, and so $G = S$ by Lemma 8.4B.

(ii) Let Γ be a moiety of Ω on which G is full. Choose a moiety Δ of Ω such that $\Gamma \cap \Delta$ is a moiety of Ω and $\Gamma \cup \Delta = \Omega$. Since $Sym(\Omega)$ is transitive on the set of moieties of Ω, there exists $x \in Sym(\Omega)$ such that $\Delta = \Gamma^x$. Now Γ and Δ are both full for $\langle G, x \rangle$ and so $\langle G, x \rangle = S$ by part (i). Finally, Exercise 8.5.3 shows that this implies that G is contained in a maximal subgroup of S. □

We next consider chains of subgroups in $Sym(\Omega)$. By a *chain of subgroups* in a group G we shall mean a family $\{H_\lambda\}_{\lambda\in\Lambda}$ of (distinct) subgroups of G indexed by a totally ordered set Λ such that $H_\lambda < H_\mu$ whenever $\lambda, \mu \in \Lambda$ and $\lambda < \mu$. The *length* of the chain is simply the cardinality of Λ. We are interested in bounds on the lengths of chains of subgroups in the symmetric groups.

If Ω is finite of size n, say, then the length of every chain of subgroups in $Sym(\Omega)$ is trivially bounded by $(\log n!)/(\log 2) \sim (n \log n)/(\log 2)$. A more careful argument shows that the length is bounded by a constant multiple of n, and this bound has been made sharp; Cameron et al. (1989).

Exercises

8.5.4 Show that there exists a constant $C > 0$ such that every chain of subgroups in S_n has length at most Cn. [*Hint:* Let M be the largest subgroup not containing A_n in the chain. If M is primitive, use Theorem 5.6B, and otherwise apply induction on degree.]

8.5.5 Show that, whenever $n > 1$ is a power of 2, there is a chain of proper subgroups in S_n of length $(3n - 4)/2$.

The situtation for the infinite symmetric groups appears to be quite different.

Theorem 8.5A. *Let $S := Sym(\Omega)$ where Ω is infinite. If $\{H_\lambda\}_{\lambda\in\Lambda}$ is a chain of proper subgroups of S such that $\bigcup_{\lambda\in\Lambda} H_\lambda = S$. Then:*
(i) $|\Lambda| > |\Omega|$; *and*
(ii) *for some $\mu \in \Lambda$, $FSym(\Omega) \leq H_\mu$, and so H_μ is highly transitive.*

PROOF. (i) The proof is a nice example of a diagonal argument. We shall first show that no H_λ can be full on any moiety. Indeed, otherwise, Lemma 8.5A (ii) shows that $S = \langle H_\mu, x\rangle$ for some $\mu \in \Lambda$ and some $x \in S$. Then $x \in H_\nu$ for some ν, and so $S \leq \langle H_\mu, H_\nu\rangle = H_{\max(\mu,\nu)}$ contrary to the hypothesis that the H_λ are proper subgroups. Therefore, no H_λ is full on a moiety of Ω. Now suppose that $|\Lambda| \leq |\Omega|$. Then there exists a partition $\{\Omega_\lambda \mid \lambda \in \Lambda\}$ of Ω into moieties, and we can choose $z_\lambda \in Sym(\Omega_\lambda)$ such that z_λ is not induced by any element of $(H_\lambda)_{\{\Omega_\lambda\}}$ acting on Ω_λ. Let $z \in Sym(\Omega)$ be the permutation which maps each Ω_λ onto itself, and whose restriction to Ω_λ equals z_λ. Then z is not contained in any of the H_λ, and so $\bigcup_{\lambda\in\Lambda} H_\lambda \neq S$ contrary to hypothesis. Thus $|\Lambda| > |\Omega|$.

(ii) $|FSym(\Omega)| = |\Omega|$ (see Exercise 8.1.3), so there exists a subset $\Lambda' \subseteq \Lambda$ of cardinality $|\Omega|$ such that $FSym(\Omega) \subseteq \bigcup_{\lambda\in\Lambda'} H_\lambda$, and (i) shows that the latter is not equal to S. Thus there exists $\mu \in \Lambda$ such that H_μ is not contained in any H_λ ($\lambda \in \Lambda'$). Since the subgroups form a chain, this means that $H_\lambda < H_\mu$ for all $\lambda \in \Lambda'$, and so $FSym(\Omega) \leq H_\mu$ as required. □

Exercise

8.5.6 Show that any group G which is not finitely generated can be written as a union of a chain of proper subgroups.

Theorem 8.5B. *Let Ω be infinite, and $\mathbf{c} > \aleph_0$. Put $S := Sym(\Omega, \mathbf{c})$.*
(i) *If $H \leq S$ and $S = FSym(\Omega)H$, then there is a finite subset $\Delta \subseteq \Omega$ such that $S_{(\Delta)} \leq H \leq S_{\{\Delta\}}$.*
(ii) *If M is a maximal subgroup of S, then either M contains $FSym(\Omega)$ (and so is highly transitive), or $M = S_{\{\Delta\}}$ for some nonempty finite subset Δ of Ω.*

Remark. Every subgroup of the form $S_{\{\Delta\}}$ with Δ nonempty and finite is maximal in S; see Exercise 8.4.1.

PROOF. Put $S := Sym(\Omega, \mathbf{c})$ and $F := FSym(\Omega)$, and suppose that $S = FH (= HF)$ for some $H \leq S$. We shall proceed by a series of steps.

(a) We shall first show that $H \cap F \neq 1$. Assume, on the contrary, that $H \cap F = 1$. Since $\mathbf{c} > \aleph_0$, we can choose $x \in S$ such that x has exactly 2^{k-1} cycles of length 2^k $(k = 1, 2, \ldots)$ and all other cycles of length 1. Since the $2^m th$ power of a 2^k-cycle is a product of 2^m disjoint cycles of length 2^{k-m} (for $0 \leq m < k$), it is possible to choose $x_m \in S$ such that $xx_m^{-2^m}$ is a product of a finite number of cycles of lengths 2^k with $k \leq m$. Thus, for each $m \geq 1$, there exists $x_m \in S$ such that $x_m^{2^m} \in Fx$. By the hypothesis on H we can choose y and y_m in H such that $x \in Fy$ and $x_m \in Fy_m$, and then $y_m^{2^m} \in Fy$ for each m. Since we are assuming that $H \cap F = 1$, we conclude that $y = y_m^{2^m}$. However, $x^{-1}y \in F$. So $\mathrm{supp}(x^{-1}y)$ is finite, and hence there exists $r \geq 1$ such that y has cycles of length 2^r (in fact this will be true for all sufficiently large r). Then $y = y_m^{2^m}$ implies that y_m has a cycle of length 2^{m+r} and so y has at least 2^m cycles of length 2^r. Since this is true for each m, we conclude that y has infinitely many 2^r-cycles, which is impossible because $\mathrm{supp}(x^{-1}y)$ is finite. Thus the assumption that $H \cap F = 1$ has led to a contradiction; so $H \cap F = 1$ as claimed.

(b) Now consider the case where H is transitive. We shall show that in this case $H = S$.

First suppose that Δ is an infinite subset of Ω with $\Omega \setminus \Delta$ also infinite. Since S acts transitively on the set of all countable subsets of Ω, there exists $x \in S$ such that $\Delta \cap \Delta^x$ and $\Delta \setminus \Delta^x$ are both infinite. By hypothesis, $x = yu$ where $u \in F$ and $y \in H$. Then $\Delta^x \setminus \mathrm{supp}(u) \subseteq \Delta^y \subseteq \Delta^x \cup \mathrm{supp}(u)$. Since $\mathrm{supp}(u)$ is finite, this shows that $\Delta \cap \Delta^y$ and $\Delta \setminus \Delta^y$ are both infinite, and so Δ is not a block for H. Hence H has no proper infinite blocks.

On the other hand, H cannot have a system of nontrivial finite blocks. Indeed, otherwise, let Δ_i $(i = 1, 2, \ldots)$ be countably many distinct blocks from such a system. Then there exists $x \in S$ such that, for each i, $\Delta_i \cap \Delta_i^x \neq \Delta_i$ or $\emptyset$. Now $x = yu$ with $y \in H$ and $u \in F$. Since u has finite support, this implies that $\Delta_i^x = \Delta_i^y$ for infinitely many i, and then the choice of x gives a contradiction. This shows that H has no system of (finite or infinite) nontrivial blocks, and so H is primitive.

Finally, since H is primitive and $F \cap H \neq 1$ by (i), Theorem 3.3D shows that $Alt(\Omega) \leq H$. Hence $|S : H| = |FH : H| = |F : F \cap H| \leq 2$, and so $H \triangleleft S$. Thus $H = S$ by Theorem 8.1A.

(c) Finally, consider the general case. Choose $x \in S$ as a permutation with infinitely many cycles of infinite length. Then there exists $y \in H$ such that $\mathrm{supp}(x^{-1}y)$ is finite, and so y must also have cycles of infinite length. In particular, H has an orbit Γ of infinite length. The argument in (b) now shows that if $\Omega \setminus \Gamma$ were also infinite, then there would exist $y \in H$ such that $\Gamma \setminus \Gamma^y$ is infinite. Since Γ is an orbit for H, this is impossible, and so

we conclude that $\Delta := \Omega \setminus \Gamma$ is finite. Now $H = H_{\{\Delta\}} \leq S_{\{\Delta\}}$, and so $S_{\{\Delta\}} = S_{\{\Delta\}} \cap FH = F_{\{\Delta\}}H$. Since Δ is finite, the subgroup $F_{(\Delta)}H_{(\Delta)}$ has finite index in $S_{(\Delta)} \cong Sym(\Gamma, \mathbf{c})$. Thus Exercise 1.3.4, Theorem 8.1A and Exercise 8.1.5 show that $F_{(\Delta)}H_{(\Delta)} = S_{(\Delta)}$. Now applying (b) shows that $H_{(\Delta)} = S_{(\Delta)}$, and so $S_{(\Delta)} \leq H \leq S_{\{\Delta\}}$ as required.

(ii) If M does not contain $FSym(\Omega)$, then $S = FSym(\Omega)M$. The result now follows from (i). □

Theorem 8.5B (ii) shows that the infinite symmetric groups have no imprimitive maximal subgroups. It also shows that the (intransitive) subgroup $S_{\{\Delta\}}$ is *not* a maximal subgroup of S when both Δ and $\Omega \setminus \Delta$ are infinite. The problem of describing *all* maximal subgroups of S remains open at this time. We conclude with a construction which provides one further class of maximal subgroups.

EXAMPLE 8.5.1. Let Δ be an infinite subset of Ω such that $|\Delta| < |\Omega|$, and put $S := Sym(\Omega)$. Then the *almost stabilizer* $A := \{x \in S \mid |\Delta \ominus \Delta^x| < |\Delta|\}$ is a maximal subgroup of S. (We are using $\ominus$ to denote symmetric difference of the two subsets.)

Indeed, clearly A is a subgroup of S and $A \neq S$. In order to show that A is maximal, we have to show that, for each $x \notin S \setminus A$, $G := \langle A, x\rangle = S$. Since $x \notin A, |\Delta \ominus \Delta^x| = |\Delta|$ so, replacing x by x^{-1} if necessary, we may assume that $|\Delta \setminus \Delta^x| = |\Delta|$. Since $|\Delta^x \cap \Delta| \leq |\Delta| = |\Delta \setminus \Delta^x|$ and $|\Delta^x \setminus \Delta| \leq |\Delta| < |\Omega \setminus (\Delta \cup \Delta^x)|$, and the sets $\Delta^x \cap \Delta$ and $\Delta^x \setminus \Delta$ are disjoint, we can find $z \in S_{\{\Delta\}} \leq A$ such that $(\Delta^x \cap \Delta)^z \subseteq \Delta \setminus \Delta^x$ and $(\Delta^x \setminus \Delta)^z \subseteq \Omega \setminus (\Delta \cup \Delta^x)$. Then $\Delta^{xz} \cap \Delta^x = \emptyset$, and so $y := xzx^{-1} \in G$ has the property that $\Delta^y \cap \Delta = \emptyset$. Put $\Gamma := \Omega \setminus \Delta$. Since $Sym(\Gamma) = S_{(\Delta)} \leq A \leq G$, we also have $Sym(\Gamma^y) = S_{(\Delta^y)} \leq G$. Moreover, $\Gamma \cup \Gamma^y = \Omega \setminus (\Delta \cap \Delta^y) = \Omega$, and $\Gamma \cap \Gamma^y = \Omega \setminus (\Delta \cup \Delta^y)$ has size $|\Omega|$. Thus $G \geq \langle Sym(\Gamma), Sym(\Gamma^y)\rangle = S$ by Lemma 8.4B. Since this is true for every $x \in S \setminus A$, therefore A is a maximal subgroup of S as asserted.

Exercises

8.5.7 Let Ω be an infinite set and $\mathbf{c}$ be an infinite cardinal. If $G \leq Sym(\Omega)$ and there exists $\Gamma \subseteq \Omega$ such that $|\Omega \setminus \Gamma| < \mathbf{c}$ and Γ is full for G, show that $Sym(\Omega) = Sym(\Omega, \mathbf{c})G$.

8.5.8 Let Ω be infinite and Δ be a moiety of Ω. Let A denote the almost stablizer of Δ in $Sym(\Omega)$. Show that there is a unique proper subgroup M of $Sym(\Omega)$ such that $A < M$, and describe this subgroup.

8.5.9 Let Ω be infinite of cardinality $\mathbf{c}$, and let $n > 1$ be an integer. Let Π be a partition of Ω into subsets of size n, and define $S_{\{\Pi\}}$ to be the subgroup of $S := Sym(\Omega)$ consisting of all elements of S which act on Π by permuting the subsets in Π. Show that $M := Sym(\Omega, \mathbf{c})S_{\{\Pi\}}$ is a proper subgroup of S. [*Hint:* Show that M is the "almost stabilizer"

of Π in the sense that: $x \in M \iff \{\Delta \in \Pi \mid \Delta^x \notin \Pi\}$ has cardinality $< \mathbf{c}$.] (It has been proved by H.D. Macpherson that M is a maximal subgroup of S; see Brazil et al. (1994).)

8.6 Notes

- Exercise 8.1.8: See Karrass and Solitar (1956).
- Exercises 8.2.3–5: See Rotman (1995) Theorem 7.7.
- Lemmas 8.3B and 8.3C: See Neumann (1975a) and (1976). See also Segal (1974).
- Lemma 8.3D and Exercise 8.3.1: See Wiegold (1974).
- Exercise 8.3.2: See Neumann (1976).
- Theorem 8.3A: See Wiegold (1974). Part (i) is due to D. Giorgetti; see Neumann (1975a) where it is shown that every group satisfying a nontrivial law lies in $\mathcal{X}$.
- Theorem 8.4A: First announced without proof in Semmes (1981). Rediscovered and proved in Dixon et al. (1986). See also Evans (1986) and (1987) and Shelah and Thomas (1989).
- Exercise 8.4.2: See Stoller (1963).
- Exercise 8.4.3: See de Bruijn (1957).
- Sect. 8.5: Further papers relevant to Sect. 8.5 include: Shelah and Thomas (1988) and (1989), MacPherson and Praeger (1990), and Baumgartner et al. (1993).
- Exercises 8.5.4–5: See Babai (1986) and Cameron et al. (1989) for the precise bound.
- Theorems 8.5A and 8.5B: See MacPherson and Neumann (1990).
- Example 8.5.1: See Ball (1966).
- Exercise 8.5.7: The converse is proved in MacPherson and Neumann (1990) Theorem 1.2.
- Exercise 8.5.9: See Ball (1966) and Brazil et al. (1994).

9

Examples and Applications of Infinite Permutation Groups

The object of this chapter is to give a selection of examples of infinite permutation groups, and a few of the ways in which permutation groups can be used in a more general context. For example, we give a criterion of Serre for a group to be free which leads to a classic theorem on free groups due to J. Nielson and O. Schreier, and give a construction due to N. D. Gupta and S. Sidki of an infinite p-group which is finitely generated. What makes these constructions manageable is that the underlying set on which the groups act have certain relational structures. The most symmetric of these structures (the ones with the largest automorphism groups) are the homogeneous structures; of these the countable universal graph is an especially interesting and well-studied example.

9.1 The Construction of a Finitely Generated Infinite p-group

In 1902 W. Burnside proposed the following question. Suppose that e and n are fixed positive integers. Is it true that every group of exponent e which can be generated by n elements is of finite order? If so, can this order be bounded by a function of n and e? (Recall that a group G has *exponent* e if $x^e = 1$ for all $x \in G$.)

This problem has turned out to be very deep. Although a lot is now known about finitely generated groups of finite exponent (now known as *Burnside groups*), there are still very hard open questions.

Let F_n be the free group on n generators and let $R_{n,e}$ denote the normal subgroup of F_n which is generated by the set $\{x^e \mid x \in F_n\}$. Then $B(n, e) := F_n/R_{n,e}$ is called the *free n-generator Burnside group of exponent e*. If G is any group of exponent e which can be generated by n elements, then by general properties of free groups, there is a homomorphism φ of F_n onto G, and evidently $R_{n,e} \leq \ker \varphi$. Thus $G \cong F_n/\ker \varphi$ is a homomorphic image of the free n-generator $B(n, e)$.

Burnside's questions may then be refined to: Is $B(n, e)$ finite (for specified n and e); and do the finite homomorphic images of $B(n, e)$ have orders bounded by a function of n and e? These are known as the *Burnside Problems*: the *General* and *Restricted Burnside Problems*, respectively. Of course, if there is a positive answer to the General Problem, then that immediately gives a positive answer to the Restricted Problem.

It has been shown that $B(n, e)$ is finite for some small values of e: for $e \leq 3$ by Burnside in 1902, for $e = 4$ by Sanov in 1940 and for $e = 6$ by Hall in 1958. Then, in 1968, there appeared a long and intricate proof by Novikov and Adian (1968) which showed that $B(n, e)$ is infinite for all $n \geq 2$, provided e is sufficiently large and odd (the result had been announced nine years earlier). A less precise, but technically simpler proof of this result was given by Ol'shanskii (1982). Since then some results about the case where e is even have also been proved. However, there are still many cases where the General Burnside Problem has not been settled; for example, it is not known whether or not $B(2, 5)$ is finite. [See Adian(1979)].

On the other hand, in 1956, P. Hall and G. Higman showed that the answer to the Restricted Burnside Problem is always positive provided that it is positive whenever e is a prime power (actually their proof required a property of finite simple groups which is a consequence of the later classification of finite simple groups). A complete positive solution of the Restricted Burnside Problem was finally obtained after A.I. Kostrikin settled the case of prime exponent in 1959, and Zelmanov (1991a) and (1991b) settled the case of general prime power exponent.

These results are all very deep. A simpler, but still interesting question, is whether there exist infinite finitely generated groups in which each element has p-power order for some fixed prime p, but where the orders of the elements are not assumed to be bounded. Of course, the result of Novikov and Adian shows that $B(n, p)$ is an example of such a group for any sufficiently large prime p. However, much more elementary examples exist. The earliest example is due to Golod (1964), and a simple construction of a 2-group with this property was given by Grigorchuk (1980). The construction which we give here is due to Gupta and Sidki (1983) and applies to all primes.

Our objective is to construct an infinite p-group which is generated by two permutations of an appropriate set. We shall go through the construction in detail for the case where p is an odd prime, and leave the modifications necessary for $p = 2$ to the exercises.

Let p be a fixed odd prime, and let Ω denote the set of all (finite) strings of the symbols $\mathbb{Z}/p\mathbb{Z}$ which we shall write $\{0, 1, \ldots, p-1\}$. Thus, for $p = 3$, typical strings might look like: 10220 or 000210222, as well as the empty string of length 0. Writing 0^r to denote the string consisting of r zeros ($r \geq 0$), we define two permutations t and z on Ω as follows.

(i) For any string of the form $i\omega$: $(i\omega)^t := (i+1)\omega$. In other words, if the string starts with i followed by a substring ω (possibly of length 0), then t changes the first symbol to $(i+1)$ and leaves the rest of the string unchanged. The empty string is left fixed by t.
(ii) For any string of the form $0^r ij\omega$ with $i \neq 0$: $(0^r ij\omega)^z := 0^r i(i+j)\omega$. In other words, z changes the first symbol following the first nonzero symbol, and leaves all other symbols unchanged; the empty string and strings entirely of zeros or of zeros followed by one nonzero symbol are left fixed by z.

Note that both t and z leave the lengths of strings invariant, so all orbits of $\langle t, z\rangle$ are finite.

Theorem 9.1A. *The group $G := \langle t, z\rangle$ is an infinite group in which each element has order a power of p.*

PROOF. We shall prove the result for the case where p is odd and leave the modifications necessary for the case $p = 2$ as an exercise (Exercise 9.1.3).

First observe that it follows at once from the definitions that z and t each have order p. Define $S := \{s_h := t^{-h}zt^h \mid h = 0, 1, \ldots, p-1\} \subseteq G$, and put $H := \langle S\rangle$. The subsets $\Omega_k := \{k\omega \mid \omega \in \Omega\}$ $(k = 0, 1, \ldots, p-1)$ are H-invariant and form a partition of Ω; in particular, $t \notin H$ and so $H \neq G$. Since it is clear that $H \lhd G$ and that $G = \langle H, t\rangle$, we conclude that G/H has order p.

A simple calculation shows that for any string $k\omega \in \Omega_k$ we have:

(9.1) $\qquad (k\omega)^{s_h}$ equals $k\omega^z$ if $k = h$ and equals $k\omega^{t^{k-h}}$ otherwise.

Thus the restriction of H to Ω_0 contains the permutations $0\omega \mapsto 0\omega^z$ and $0\omega \mapsto 0\omega^t$, and so contains a copy of G. Since $H < G$, this implies that G must be infinite.

We now turn to the proof that each element of G has p-power order. We know that $H = \langle S\rangle \lhd G, G = \langle H, t\rangle$, and that t and each of the elements in S has order p. Thus each $x \in G$ can be written in at least one way in the form

$$x = t^u s_{i_1} \cdots s_{i_m} \tag{9.2}$$

where m is chosen as small as possible and $0 \leq u <$ p. We shall proceed by induction on m to prove that x is a p-element. Since t has order p, x is a p-element when $m = 0$. Thus suppose that $m > 0$, and that the result is true for all elements x which can be expressed in the form (9.2) with a product of fewer than m of the s_i. We consider two cases.

First suppose that $u = 0$. In this case $x \in H$ and so it leaves each Ω_i invariant. Moreover, (9.1) shows that for each string $k\omega \in \Omega_i$ we have $(k\omega)^x = k\omega^w$ where w has the form $t^v s_{j_1} \cdots s_{j_n}$ when n of the i_h in the product for x are equal to k. Thus, if the subscripts i_h in (9.2) are not all equal, then induction shows that, for each k, the restriction of x to Ω_k is

a p-element, and so x is a p-element. On the other hand, if all i_h have the same value, say i, then $x = s_i$ and so x has order dividing p. This proves the induction step in the case $u = 0$.

The other possibility is that $0 < u < p$. In this case put $y := s_{i_1} \cdots s_{i_m}$. Then

$$x^p = (t^u y)^p = t^{up} \cdot t^{-u(p-1)} y t^{u(p-1)} \cdots y = t^u y t^{-u} \cdot t^{2u} y t^{-2u} \cdots y$$

since $t^p = 1$. Since $p \nmid u$, the exponents $u, 2u, \ldots, 0$ which appear in the expression above for x^p correspond to a full set of residue classes modulo p. Now

$$t^r y t^{-r} = t^r s_{i_1} t^{-r} \cdot t^r s_{i_2} t^{-r} \cdots t^r s_{i_m} t^{-r} = s_{i_1} s_{i_2} \cdots s_{i_m}$$

where the indices in the product on the right should be read modulo p. Hence x^p can be written as a product of pm terms of the form s_i $(0 \leq i < p)$. Since the exponents $u, 2u, \ldots, 0$ correspond to a full set of residue classes modulo p, each s_i occurs as a factor exactly m times. We now apply (9.1) to see that for each k we have: $(k\omega)^{x^p} = k\omega^w$ where w (depending on k) is a product consisting of pm factors which are either powers of t or equal to z. Moreover, z occurs as a factor exactly m times and the total power to which t occurs is $v := m(1 + 2 + \cdots + p - 1) = m(p-1)p/2$. By using identities of the form $s_i t^r = t^r s_{i+r}$ (indices taken modulo p), we can rewrite this product for w in the form $w = t^v s_{j_1} s_{j_2} \cdots s_{j_m}$ where $t^v = 1$ because $p \mid v$ (this is where the fact that p is odd is used). Now the first case of the proof of the induction step applies, and we can conclude that w has p-power order. Since this is true for each k, we conclude that x^p, and hence x itself, is a p-element. This completes the proof of the induction step in the second case, and the theorem is proved. □

Exercises

9.1.1 Show that the orders of the elements in G are not bounded (so G is not a homomorphic image of a Burnside group).

9.1.2 Show that G is residually finite.

9.1.3 The construction above does not work for $p = 2$ (why?). To obtain the corresponding theorem for $p = 2$, take Ω as the set of all finite strings over $\mathbb{Z}/4\mathbb{Z}$. Define t as above, but modify the definition of z as follows: for any string of the form $0^r ij\omega$ with $i \neq 0$: $(0^r ij\omega)^z := 0^r i(i+j)\omega$ if $i = 1$ or 3, and $(0^r 2j\omega)^z = 0^r 2j\omega$.

9.2 Groups Acting on Trees

Recall that a *tree* is a connected graph with no nontrivial circuits (see Section 2.3). Alternatively, a graph $\mathcal{T}$ is a tree if for every pair α, β of vertices there exists a unique simple path from α to β in $\mathcal{T}$: a finite sequence

$\alpha = \alpha_0, \alpha_1, \ldots, \alpha_k = \beta$ of distinct vertices such that each of the k consecutive pairs α_i, α_{i+1} of vertices are adjacent in $\mathcal{T}$. In the latter case we shall write $d(\alpha, \beta) := k$, and say that α and β have *distance* k in $\mathcal{T}$. It may be immediately verified that d defines a metric on the set Ω of vertices of $\mathcal{T}$. For subsets Γ and Δ of Ω and a point α, $d(\alpha, \Delta)$ will denote the minimum distance from α to Δ, and $d(\Gamma, \Delta)$ will denote the minimum distance from a point in Γ and to a point in Δ.

If $\mathcal{T}$ is a finite tree then the automorphism group of $\mathcal{T}$ either fixes a vertex or interchanges two adjacent vertices (see Exercise 9.2.4); the groups which arise are not particularly interesting. We shall be considering infinite trees, but often assume that the tree is *locally finite*, namely, that each vertex has finite degree. An infinite, locally finite tree has countably many vertices (see Exercise 2.3.1).

Exercises

9.2.1 Show that if $\mathcal{T}$ is a tree with vertex set Ω, then the group $\mathrm{Aut}(\mathcal{T})$ of permutations of Ω which preserve the graph structure is also the set of all permutations of Ω which preserve the distance d defined above.

9.2.2 Describe all trees with at most 5 vertices, and calculate the automorphism group for each of these trees.

9.2.3 Define an relation on the vertives of a tree $\mathcal{T}$ by $\alpha \equiv \beta \iff d(\alpha, \beta)$ is even. Show that this is an equivalence relation and that it is invariant under every automorphism of the tree.

9.2.4 Let $\mathcal{T}$ be a finite tree with vertex set Ω. Define the function f on the vertices by $f(\alpha) = \sum_{\beta \in \Omega} d(\alpha, \beta)$. Show that f takes its minimum value either at a unique vertex or at two adjacent vertices. Hence prove that $\mathrm{Aut}(\mathcal{T})$ fixes a vertex or an edge. (Alternatively, this vertex or edge is the "centre" of every longest path in the tree.)

9.2.5 Suppose that $\mathcal{T}$ is a tree with an automorphism x of order 2. Show that x either fixes a vertex or interchanges two adjacent vertices. [*Hint:* If $\alpha \neq \alpha^x$, then x maps the unique path from α to α^x onto itself.]

If F is a free group on a set R then the Cayley graph $\mathcal{T} := \mathrm{Cayley}(F, R)$ is a tree (see Exercise 2.3.11). Each vertex has degree $|R \cup R^{-1}|$, and so if $|R|$ (the *rank* of G) is finite, then $\mathcal{T}$ locally finite. The action of F on the vertex set F of $\mathcal{T}$ by right multiplication preserves the adjacency property, and so we can embed F into $\mathrm{Aut}(\mathcal{T})$ (see Exercise 2.3.10). It is easily seen, that in this action only the trivial element fixes a vertex or reverses an edge of $\mathcal{T}$. Our first result, due to J.P. Serre, shows that this latter property characterizes free groups.

To clarify the statement of the theorem we shall say that a group G acting as a group of automorphisms on a tree $\mathcal{T}$ acts *freely* if the only element of G to fix a vertex or reverse an edge of $\mathcal{T}$ is the trivial element. Exercise 9.2.5 shows that if a group acts freely on a tree then the group

cannot contain an element of order 2. The following theorem gives a much stronger statement. Serre's original proof shows that the conclusion remains true when the hypothesis of "locally finite" is dropped.

Theorem 9.2A. *Any group which acts freely on a locally finite tree is a free group.*

PROOF. Let G be a group acting freely on a locally finite tree $\mathcal{T}$, and let Ω be the set of vertices of $\mathcal{T}$. Fix a vertex $\omega \in \Omega$. Since $\mathcal{T}$ is locally finite, there are only finitely many vertices at any given distance from ω. Thus there exists an enumeration $\omega_0 = \omega, \omega_1, \omega_2, \dots$ of Ω such that $d(\omega, \omega_k) \leq d(\omega, \omega_{k+1})$ for all k. We define $\Gamma \subseteq \Omega$ recursively by the conditions: $\omega = \omega_0 \in \Gamma$; and, for each $k \geq 1$, $\omega_k \in \Gamma$ if and only if ω_k is adjacent to one of the points $\omega_j \in \Gamma$ with $j < k$, but does not lie in the G-orbit of any of these points. In particular, the subgraph induced on Γ is connected, and so is a subtree of $\mathcal{T}$.

The construction of Γ shows that Γ does not contain more than one point from each G-orbit in Ω. We claim, in fact, that Γ contains exactly one vertex from each G-orbit, and that each G-orbit Δ is represented by a point $\delta \in \Gamma$ satisfying $d(\omega, \delta) = d(\omega, \Delta)$. We shall prove this by induction on $m := d(\omega, \Delta)$. The claim is true for $m = 0$ since then $\Delta = \omega^G$ and $\omega = \omega_o \in \Gamma$. Therefore suppose that Δ is an orbit with $m = d(\omega, \Delta) > 0$ and that the claim holds for all orbits with smaller distance to ω. Choose $\alpha \in \Delta$ with $d(\omega, \alpha) = m$. Then α is adjacent to some vertex β, say, with $d(\omega, \beta) = m - 1$. By induction, there exists $x \in G$ such that $\beta^x \in \Gamma$ and $d(\omega, \beta^x) \leq d(\omega, \beta)$. Then α^x is adjacent to β^x and

$$m = d(\omega, \Delta) \leq d(\omega, \alpha^x) \leq d(\omega, \beta^x) + 1 \leq d(\omega, \beta) + 1 = m.$$

Hence $d(\omega, \alpha^x) = d(\omega, \Delta)$. Suppose $\alpha^x = \omega_k$ in the enumeration of Ω. Since α^x is adjacent to β^x and $\beta^x \in \Gamma$, the construction of Γ shows that $\omega_k \in \Gamma \cap \Delta$ unless $\omega_j \in \Gamma \cap \Delta$ for some $j < k$. In the latter case $d(\omega, \Delta) \leq d(\omega, \omega_j) \leq d(\omega, \omega_k)$ by the enumeration of Ω. Thus in either case Γ contains a representative of Δ at minimum distance from ω. This proves the induction step, and the claim is proved.

We next note that $\Gamma^x \cap \Gamma^y = \emptyset$ whenever $x, y \in G$ are distinct. Indeed, if $\Gamma^x \cap \Gamma^y \neq \emptyset$, then there exist $\gamma, \delta \in \Gamma$ such that $\gamma^x = \delta^y$. Since Γ contains only one point from each orbit, this shows that $\delta = \gamma$, and so $xy^{-1} \in G_\delta$. But G acts freely on $\mathcal{T}$, so must have $x = y$. Thus the sets Γ^x $(x \in G)$ are pairwise disjoint. Since Γ is a set of representatives of G-orbits on Ω, this shows that the family of sets Γ^x $(x \in G)$ is a partition of Ω.

Now define $T := \{t \in G \mid d(\Gamma, \Gamma^t) = 1\} = T^{-1}$. Since G acts freely, G contains no elements of order two, so we can write $T = R \cup R^{-1}$ as a union of disjoint sets. We shall show that R is a set of free generators for G. To do this we must show that R generates G, and that there are no nontrivial relations between the elements of R.

To show that R generates G we proceed to show that each $x \in G$ lies in $\langle T \rangle = \langle R \rangle$ by induction on $m := d(\Gamma, \Gamma^x)$. If $m = 0$, then $\Gamma \cap \Gamma^x \neq \emptyset$, and so $x = 1$ from above. On the other hand, if $m > 0$, then for some $\alpha \in \Omega$ we have $d(\Gamma, \alpha) = 1$ and $d(\alpha, \Gamma^x) = m - 1$. Then for some $t \in T$ we have $\alpha \in \Gamma^t$ and $d(\Gamma, \Gamma^{xt^{-1}}) = d(\Gamma^t, \Gamma^x) \leq m - 1$. Hence $xt^{-1} \in \langle T \rangle$ by induction, and so we conclude that $x \in \langle T \rangle$ as required.

Finally we show that the elements in R satisfy no nontrivial relations. Otherwise, for some $n \geq 2$, there would be a product $t_1 t_2 \cdots t_n = 1$ with each $t_k \in T$ and such that $t_k t_{k+1} \neq 1$ for $1 \leq k < n$ and $t_n t_1 \neq 1$. Put $x_k := t_k \dots t_n$ $(1 \leq k \leq n)$ and $x_{n+1} := 1$. Then $d(\Gamma^{x_k}, \Gamma^{x_{k+1}}) = d(\Gamma^{t_k}, \Gamma) = 1$ for each k, and so there is a path in $\mathcal{T}$ of the form:

$$\omega^{x_{n+1}} = \omega, \Pi_n, \omega^{x_n}, \Pi_{n-1}, \omega^{x_{n-1}}, \Pi_{n-2}, \dots, \Pi_1, \omega^{x_1}$$

where Π_k is a list of points such that Π_k, ω^{x_k} is a path in the subtree Γ^{x_k} from a vertex in this subtree adjacent to $\omega^{x_{k+1}}$ to the vertex ω^{x_k}. Since $x_{n+1} = x_1 = 1$, this gives a circuit in $\mathcal{T}$, which is impossible because $\mathcal{T}$ is a tree. Hence there are no nontrivial relations between the elements of R, and so we have proved that R is a set of free generators for G. This proves the theorem. □

Corollary 9.2A. *If F is a free group of finite rank, then every subgroup of F is also free (possibly of infinite rank).*

PROOF. Suppose that R is a set of free generators for F. As we noted above, Cayley(F, R) is a locally finite tree on which F (and hence every subgroup of F) acts freely. Now the theorem applies. □

Again the result is true without the hypothesis of finite rank. Moreover, it can be shown that if F is free of rank r, then any subgroup of index h in F has rank $h(r-1)+1$ [see Serre (1980)]. We use this fact in the next section.

We now consider more general actions of groups on trees. To do this we introduce the concept of a line in a graph. The *standard line* is the tree with vertex set $\mathbb{Z}$ such that $i, j \in \mathbb{Z}$ are adjacent if and only if $|i - j| = 1$. Similarly the *standard half-line* is the tree with the same adjacency rule on the vertex set $\mathbb{N}$. More generally, a *line* (respectively, *half-line)* in a graph $\mathcal{G}$ is a subset Λ of vertices of $\mathcal{G}$ such that the subgraph induced on Λ is isomorphic to the standard line (half-line).

A *translation* of a graph $\mathcal{G}$ *along* a line Λ is an automorphism x of $\mathcal{G}$ which fixes Λ setwise. In the case that $\mathcal{G}$ is a tree and d is the corresponding metric, then $m := d(\alpha, \alpha^x)$ is constant for $\alpha \in \Lambda$ (see Exercise 9.2.7 below). In this case we say that x is a translation by m along Λ, and x is a *nontrivial* translation if $m > 0$.

We shall say that a vertex γ in a tree lies *between* vertices α and β if γ lies on the simple path from α to β.

Exercises

9.2.6 If x is a translation of a tree $\mathcal{T}$ along a line Λ, and $\alpha \in \Lambda$, show that all vertices on the simple path from α to α^x in $\mathcal{T}$ lie in Λ.

9.2.7 If x is a translation of a tree along a line Λ show that $m := d(\alpha, \alpha^x)$ is constant for all $\alpha \in \Lambda$. If β is a vertex not in Λ, show that $d(\beta, \beta^x) > m$.

9.2.8 Let α and β be adjacent vertices in a tree, and let γ be a vertex distinct from both of these. Show that either α lies between β and γ, or β lies between α and γ.

9.2.9 Let Λ be an infinite set of vertices from the tree $\mathcal{T}$. Show that Λ is a line if and only if the subgraph induced on Λ is connected and each vertex in Λ is adjacent to exactly two other vertices in Λ. Give a corresponding criterion for Λ to be a half-line.

9.2.10 Show that every infinite locally finite tree contains a half line starting at an arbitrary vertex.

9.2.11 Give an example of an infinite tree which contains no half-line.

There is a simple criterion for an automorphism of a tree to be a translation.

Lemma 9.2A. *Let x be an automorphism of a tree $\mathcal{T}$.*

(i) *Suppose that there exist distinct vertices α and β of $\mathcal{T}$ such that β lies between α to α^x, and that α^x lies between α and β^x. Put $k := d(\alpha, \alpha^x)$. Then x is a translation of $\mathcal{T}$ by k along some line Λ containing the points α and β.*

(ii) *Any translation along more than one line acts trivially on both lines.*

PROOF. (i) Let $\alpha_0 = \alpha, \alpha_1, \dots, \alpha_k = \alpha^x$ be the simple path from α to α^x in $\mathcal{T}$. Note that $\beta = \alpha_r$ for some r with $0 < r \leq k$ by hypothesis, and so $\alpha \neq \alpha^x$. Now define α_n for all $n \in \mathbb{Z}$ by writing $\alpha_{ik+j} := \alpha_j$ for $0 \leq j < k$ and $i \in \mathbb{Z}$. Since $x \in \mathrm{Aut}(\mathcal{T})$, α_n is adjacent to α_{n+1} for all $n \in \mathbb{Z}$. On the other hand $\Lambda := \{\alpha_n \mid n \in \mathbb{Z}\}$ is set-invariant under x. It remains to show the α_n are distinct vertices; then Λ will be a line and x will be a translation by k along Λ.

Suppose on the contrary that $\alpha_m = \alpha_n$ for some $m < n$, and choose m and n so that $n - m$ is as small as possible. Since $\alpha_m = \alpha_{m+ki}$, we can also suppose that $0 \leq m < k$, and then $n > k$ because $\alpha_0, \alpha_1, \dots, \alpha_k$ are distinct. Now the two paths $\alpha_m, \alpha_{m+1}, \dots, \alpha_{k-1}, \alpha_k$ and $\alpha_m = \alpha_n, \alpha_{n-1}, \dots, \alpha_{k+1}, \alpha_k$ from α_m to α_k are simple by the minimal choice of $n - m$, and so must be identical because $\mathcal{T}$ is a tree. In particular, $\alpha_{k-1} = \alpha_{k+1}$. However, $\beta = \alpha_r$ with $0 < r \leq k$, and so $\beta^x = \alpha_{r+k}$ lies between α_{k+1} and α_{2k}. Hence the path $\alpha = \alpha_0, \alpha_1, \dots, \alpha_{k-1} = \alpha_{k+1}, \dots, \alpha_{r+k} = \beta^x$ from α to β^x does not pass through $\alpha^x = \alpha_k$ because both $\alpha_0, \alpha_1, \dots, \alpha_k$ and its x-image $\alpha_k, \alpha_{k+1}, \dots, \alpha_{2k}$ are simple paths. Since some subpath of this path gives the simple path from α to β^x,

this contradicts the hypothesis that α^x lies between α and β^x. Hence we conclude that the α_n are all distinct as required, and (i) is proved.

(ii) Suppose that x is a translation by $m > 0$ along a line Λ and also a translation along a different line Λ'. Since Λ and Λ' are orbits for x, they are necessarily disjoint, so $d(\Lambda, \Lambda') > 0$. Choose $\alpha \in \Lambda$ and $\beta \in \Lambda'$ such that $d(\alpha, \beta) = d(\Lambda, \Lambda')$. Except for α and β, the vertices on the simple path from β to α must all lie outside of $\Lambda \cup \Lambda'$. The simple path from α to α^x lies in Λ (see Exercise 9.2.6), and so there is a simple path from β to α^x passing through α on which β is the only vertex in Λ'. However, a similar argument shows that there is a simple path from β to α^x passing through β^x on which the only vertex in Λ is α^x. Since these two paths must be the same, we must have $\alpha = \alpha^x$ contrary to the hypothesis that $m > 0$. This proves (ii). □

This lemma forms the basis of the following classification of automorphisms of trees due to Tits (1970).

Theorem 9.2B. *Let $\mathcal{T}$ be a tree. Then each automorphism x of $\mathcal{T}$ satisfies exactly one of the following conditions:*

(i) *$\Gamma := \mathrm{fix}(x) \neq \emptyset$ and the induced subgraph on Γ is a subtree;*
(ii) *x interchanges a pair of adjacent vertices in $\mathcal{T}$;*
(iii) *x is a translation by m along some line Λ with $m > 0$, and $d(\alpha, \alpha^x) > m$ for all $\alpha \notin \Lambda$.*

Proof. It is evident that if (iii) holds then neither (i) nor (ii) can hold. On the other hand, suppose that x fixes a vertex γ, and that α and β are adjacent vertices in $\mathcal{T}$. Using Exercise 9.2.8, we may assume, without loss in generality, that β lies between α and γ, and hence $d(\alpha, \gamma) = 1 + d(\beta, \gamma)$. Since x preserves the metric d, this shows that x cannot interchange α and β. Hence if (i) holds, then (ii) does not. This shows that at most one of the conditions (i)–(iii) can hold for each $x \in \mathrm{Aut}(\mathcal{T})$. We now show that at least one will hold.

First note that, if α and β are two fixed points in $\mathcal{T}$, then the simple path from α to β is mapped under x again onto a simple path from α to β. By the uniqueness of this path, each of the points on the path must be fixed by x. This shows that if $\mathrm{fix}(x) \neq \emptyset$, then the subgraph induced on the fixed points is connected and hence a subtree (and so (i) holds).

Now assume that $x \in \mathrm{Aut}(\mathcal{T})$ has no fixed points and does not interchange any pair of adjacent vertices. Then neither (i) nor (ii) holds; we must prove that (iii) holds. Choose a vertex α such that $m := d(\alpha, \alpha^x)$ is as small as possible, and let $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \alpha^x$ be the simple path from α to α^x in $\mathcal{T}$. Since x has no fixed point, $m > 0$, and so we can define $\beta := \alpha_1 \neq \alpha$. Since $d(\beta, \beta^x) \geq m$ by the choice of α, β^x cannot lie between β and α^x. On the other hand, $d(\alpha^x, \beta^x) = d(\alpha, \beta) = 1$, so Exercise 9.2.8 shows that α^x lies between β and β^x. Now Lemma 9.2A applies and we

conclude that x is a translation by m along some line Λ containing α and β. Finally, by the choice of m, $d(\gamma, \gamma^x) \geq m$ for all vertices γ; so it remains to show that $d(\gamma, \gamma^x) = m$ implies $\gamma \in \Lambda$. However, if $d(\gamma, \gamma^x) = m$, then the argument above with γ in place of α shows that x is a translation along some line Λ' containing γ. Now Lemma 9.2A (ii) shows that $\Lambda' = \Lambda$, and so $\gamma \in \Lambda$ as required. This completes the proof of the theorem. □

Exercises

9.2.12 Give an example of a translation $x \neq 1$ of a tree which leaves more than one line invariant.

9.2.13 Suppose that x and y are automorphisms of a tree $\mathcal{T}$, and that each interchanges a pair of adjacent vertices. If these pairs are disjoint, show that xy is a translation.

The set of vertices of degree 1, the *leaves*, of a tree is invariant under the automorphism group of the tree. An infinite tree may also contain lines (or half-lines) which do not have terminal vertices. In a certain sense, the extremites of lines of a tree also constitute an invariant set. Define an equivalence relation on half-lines by taking half-lines Λ_1 and Λ_2 to be equivalent if the intersection $\Lambda_1 \cap \Lambda_2$ is also a half-line. So half-lines are equivalent if they are eventually the same sequence of vertices. An *end* is an equivalence class of half-lines under this relation. The full automorphism group of $\mathcal{T}$ induces a permutation action on the set $\Delta(\mathcal{T})$ of ends of $\mathcal{T}$.

The group induced on the ends of $\mathcal{T}$ can have interesting properties. For each $k \geq 2$, there is an essentially unique tree $\mathcal{T}_k$ which has a countable vertex set and such that every vertex has degree k (Exercise 9.2.14). $\mathcal{T}_k$ is the *countable k-regular tree*. (The tree $\mathcal{T}_3$ was introduced in Example 1.5.4.) The set of ends $\Delta_k := \Delta(\mathcal{T}_k)$ is uncountable and the group induced on Δ_k by $G_k := \mathrm{Aut}(\mathcal{T}_k)$ is faithful and 3-transitive but not 4-transitive (Exercises 9.2.18 and 9.2.19). It can be shown that, if $k \neq m$ then G_k is not isomorphic to G_m [see Znoiko (1977) and Möller (1991)].

Exercises

Let $k \geq 2$.

9.2.14 Show that there exists a countably infinite tree $\mathcal{T}_k$ in which each vertex has degree k, and that any two such trees are isomorphic.

9.2.15 If $\mathcal{U}$ and $\mathcal{V}$ are finite subtrees of $\mathcal{T}_k$ and $\phi : \mathcal{U} \rightarrow \mathcal{V}$ is an isomorphism, show that there exists $\psi \in \mathrm{Aut}(\mathcal{T}_k)$ such that ϕ is the restriction of ψ to $\mathcal{U}$. In particular, $\mathrm{Aut}(\mathcal{T}_k)$ acts transitively on both the vertex set and the set of edges of $\mathcal{T}_k$.

9.2.16 Show that $\mathrm{Aut}(\mathcal{T}_k)$ acts imprimitively on the vertex set Ω with two blocks Ω_1 and Ω_2, say, where α and β lie in the same block if and only if $d(\alpha, \beta)$ is even; and that $\mathrm{Aut}(\mathcal{T}_k)_{\{\Omega_1\}}$ acts primitively on each of the blocks.

9.2.17 Suppose that B_1, B_2 are two distinct ends of a tree $\mathcal{T}$. Show that there is a unique line Λ in $\mathcal{T}$ such that the two half-lines derived from splitting Λ at any vertex lie one in B_1 and the other in B_2. (Thus any two distinct ends are "joined" by a line of $\mathcal{T}$.)

9.2.18 Suppose that $\mathcal{T}$ is a tree in which every vertex has degree at least 3. Show that the set $\Delta(\mathcal{T})$ of ends is uncountable.

9.2.19 Show that the automorphism group G_k of the k-regular graph $\mathcal{T}_k$ acts faithfully on the set Δ_k of ends and is 3-transitive but not 4-transitive.

9.2.20 Describe the orbits of G_k on the set of 4-sets from Δ_k.

9.3 Highly Transitive Free Subgroups of the Symmetric Group

A finitely generated group has at most countably infinite order. Hence a transitive, finitely generated permutation group has either finite or countably infinite degree. We might wonder whether it is possible for a finitely generated group of countable degree to be highly transitive. In fact, it turns out that, in a suitable sense, almost all finitely generated groups of countable degree are both highly transitive and free [Dixon (1990)]. We shall not prove that here, but shall give a construction due to McDonough (1977) of a specific example of such a group.

EXAMPLE 9.3.1. We shall first construct a group $G = \langle x, y \rangle \leq Sym(\mathbb{Z})$ which is both highly transitive and free of rank 2. We shall then show how to derive further examples of highly transitive free groups of other ranks.

Let x be defined by $\alpha^x := \alpha + 1$ for all $\alpha \in \mathbb{Z}$, and let y be an infinite cycle in $Sym(\mathbb{Z})$ with support $\mathbb{N}$. We shall prove that under these conditions: (i) G is always highly transitive; and (ii) for a suitable choice of y, G is free of rank 2.

To prove (i) we first note that $x^n y x^{-n}$ is a cycle with support $\Omega_n := \{\alpha \in \mathbb{Z} \mid \alpha \geq -n\}$. Then a simple induction on n shows that $G_n := \langle y, xyx^{-1}, \ldots, x^n y x^{-n} \rangle$ is $(n+1)$-transitive on Ω_n for $n = 0, 1, \ldots$. Since each finite subset of $\mathbb{Z}$ is contained in all but a finite number of the Ω_n with $n \geq 0$, and $G_n \leq G$, it follows that G is k-transitive for each $k \geq 1$. Hence G is highly transitive. This proves (i).

To prove (ii) we have to construct y so that x and y satisfy no nontrivial relation. Let R denote the set of all $2k$-tuples

$$(r_1, s_1, \ldots, r_k, s_k) \tag{9.3}$$

of nonzero integers r_i, s_i with $k \geq 1$. Then x and y are free generators for G provided each of the words $w(r_1, s_1, \ldots, r_k, s_k) := x^{r_1} y^{s_1} \cdots x^{r_k} y^{s_k}$ is not equal to 1 (every relation is reducible to one of this type). Suppose that

$(r_1, s_1, \ldots, r_k, s_k) \in R$, and put $M := \sum |s_i| + 1$. For each $\alpha \in \mathbb{N}$ and any integer $r \neq 0$, we define $\Lambda(\alpha, r, M)$ to be the list $\alpha, \alpha + M, \ldots, \alpha + rM$ if $r > 0$, and to be $\alpha + |r| M, \alpha + (|r| - 1)M, \ldots, \alpha$ if $r < 0$. Then for any $\alpha_1 \in \mathbb{N}$ we define recursively $\alpha_{i+1} := \alpha_i + |r_i| M + s_i$ $(i = 1, \ldots, k)$. By the choice of M, $\alpha_1 < \alpha_2 < \ldots < \alpha_{k+1}$, and $\Lambda(\alpha_i, r_i, M)$ $(i = 1, \ldots, k)$ are disjoint lists of integers $\geq \alpha_1$. If each of the lists $\Lambda(\alpha_i, r_i, M)$ $(i = 1, \ldots, k)$ appears as consecutive elements in the cycle y, then $y^{r_i} x^{s_i}$ maps α_i onto α_{i+1}, and so $w(r_1, s_1, \ldots, r_k, s_k)$ maps α_1 onto $\alpha_{k+1} \neq \alpha_1$. In particular, for any such cycle, the word $w(r_1, s_1, \ldots, r_k, s_k) \neq 1$.

It is now clear how to construct the cycle y so that x and y satisfy no nontrivial relation. The set R of elements of the form (9.3) is countable, and so we can enumerate these elements. Then, successively, for each element of R we construct lists $\Lambda(\alpha, r, M)$ as above, such that all of the lists constructed are mutually disjoint, and so that infinitely many points in $\mathbb{N}$ do not occur in any of the lists. Finally we concatenate the lists $\Lambda(\alpha, r, M)$ on the right, and list the remaining points from $\mathbb{N}$ on the left, to obtain an infinite cycle y with support $\mathbb{N}$. From what we have proved above, each word $w(r_1, s_1, \ldots, r_k, s_k) \neq 1$, and so x and y are free generators for G. This proves (ii).

This gives a construction of a highly transitive free group of rank 2. To construct examples of other highly transitive free groups we can proceed as follows. First note that any nontrivial normal subgroup of G is also highly transitive (see Corollary 7.2A). Now by the universal property for free groups, there exists a homomorphism of the free group G onto every group which can be generated by at most two elements. Hence, mapping G (for example) onto a cyclic group shows that G has nontrivial normal subgroups of index h for each finite h and also of infinite index. It is known that any subgroup of (finite or infinite) index h in a free group of rank r is free of rank $h(r - 1) + 1$ (see Rotman (1995) Theorem 12.25). Since G is free of rank 2, this shows that G contains a highly transitive normal subgroup of rank $h + 1$ for each finite $h \geq 1$, and also a highly transitive normal subgroup of countably infinite rank.

The exercises that follow give an alternative way to construct highly transitive free groups of countably infinite rank.

Exercises

9.3.1 Suppose $G \leq Sym(\Omega)$ and N is a normal subgroup of G such that G/N is a free group of countably infinite rank. If N is highly transitive, show that there exists a highly transitive subgroup $H \leq G$ such that $G = HN$ and $H \cap N = 1$. Note that, since $H \cong G/N$, H is also free of countable rank. [*Hint:* Let $Nx_i (i = 1, 2, \ldots)$ be a set of free generators for G/N. Show that you can choose $u_i \in N$ such that $H := \langle u_i x_i \mid i = 1, 2, \ldots \rangle$ is highly transitive.]

9.3.2 Take $G := K \cdot FSym(\mathbb{N})$ where $K \leq Sym(\mathbb{N})$ is a regular representation of the free group of countable rank. The previous exercise shows that G contains a subgroup H which is highly transitive and free of countable rank. Show that each nontrivial element of H has only a finite number of fixed points.

9.4 Homogeneous Groups

A group G acting in a set Ω induces an action on the set $\Omega^{\{k\}}$ of k element subsets of Ω, for all $k \geq 1$. The group G is *k-homogeneous* if its action on $\Omega^{\{k\}}$ is transitive. An infinite group is *highly homogeneous* if it is k-homogeneous for all integers $k \geq 1$. Clearly any k-transitive group is k-homogeneous. Also if G is k-homogeneous of finite degree n then G is also $(n-k)$-homogeneous. These ideas were introduced in Sect. 2.1; we look at them more closely here. In the finite case, with a small number of well described exceptions, a k-homogeneous group is actually k-transitive (see Theorem 9.4B). In the infinite case, the property of k-homogeneity is distinct from k-transitivity, and interesting new examples arise.

EXAMPLE 9.4.1. Let $x := (1\,2\,3\,4\,5\,6\,7)$ and $y := (2\,3\,5)(4\,7\,6)$. Note that $y^{-1}xy = x^2$. Let $G = \langle x, y\rangle \leq S_7$. Then $|G| = 21$ so G is clearly not 2-transitive. However, G is 2-homogeneous. To see this note first that for any pair of distinct points α, β there exists $z \in G$ such that $\{\alpha,\beta\}^z = \{1,\gamma\}$ for some γ. If $\gamma \in \{2,3,5\}$ then $\{\alpha,\beta\}^{zy^i} = \{1,2\}$ for some i; otherwise, $\{a,\beta\}^{zy^jx} = \{1,2\}$ for some j. Thus G has a single orbit on 2-sets. For the general situation, see Exercise 2.1.11.

EXAMPLE 9.4.2. Let $G = \mathrm{Aut}(\mathbb{Q},\leq)$ be the group of all order preserving automorphisms of the rationals. Then G is highly homogeneous but is not 2-transitive (see Exercise 2.2.8). The group H of all permutations that preserve or reverse the order on $\mathbb{Q}$ contains G, so is again highly homogeneous; it is 2-transitive but not 3-transitive on $\mathbb{Q}$ (Exercise 7.1.2). The group H can be described as the group of permutations preserving a ternary *between* relation B on $\mathbb{Q}$ where B is defined by

$$(\alpha,\beta,\gamma) \in B \iff \beta < \alpha < \gamma \text{ or } \gamma < \alpha < \beta.$$

EXAMPLE 9.4.3. Let Ω be the points on the unit circle, and let G be the group of all permutations of Ω that preserve the *separation* relation S where $(\alpha,\beta,\gamma,\delta) \in S$ when a shortest path from α to β along the circle runs through exactly one of γ and δ. The group preserving this relation is highly homogeneous and 3-transitive but not 4-transtive. We can make this an example of countable degree by replacing Ω by the set of all roots of unity.

Exercises

9.4.1 Verify the assertions of Examples 9.4.2 and 9.4.3.

9.4.2 Let Ω be the set of complex roots of unity and S be the separation relation. Fix one point α and define a relation R on $\Omega \setminus \{\alpha\}$ by $(\beta, \gamma, \delta) \in R \iff (\alpha, \beta, \gamma, \delta) \in S$. Show that $\Omega \setminus \{\alpha\}$ with this relation is isomorphic to $\mathbb{Q}$ with the between relation.

9.4.3 Let $G = \mathrm{Aut}(\Omega, \leq)$ be the full automorphism group of a totally ordered set $(\Omega, \leq)$. If G is 2-homogeneous, show that Ω is infinite and G is highly homogeneous.

9.4.4 Under the hypotheses of Exercise 9.4.4, show that $(\Omega, \leq)$ is dense.

9.4.5 Show that the group $PGL_2(8)$ in its action on the projective line $PG_1(8)$ is k-homogeneous for each $k = 1, \ldots, 9$.

Taking a more general setting for the moment, we consider the action of G on k-sets. Denote by $f_k = f_k(G)$ the number of orbits of G on $\Omega^{\{k\}}$. The first theorem establishes the remarkable fact that the series $f_1, f_2, \ldots$ is monotonic (up to $|\Omega|/2$ in the finite case). Since G is k-homogeneous if and only if $f_k = 1$, it follows that a k-homogeneous group is also $(k-1)$-homogeneous. In particular, a 2-homogenous group is always transitive. The proof we give comes from Cameron (1976) and is based on the following lemma.

Let Γ and Δ be nonempty sets and suppose that $\Lambda \subseteq \Gamma \times \Delta$ has the property:

(9.4) for all $\delta \in \Delta$, the set $\{\gamma \in \Gamma \mid (\gamma, \delta) \in \Lambda\}$ is finite.

Let $\mathrm{Fun}(\Gamma, \mathbb{Q})$ and $\mathrm{Fun}(\Delta, \mathbb{Q})$ denote the vector spaces over $\mathbb{Q}$ consisting of all functions from Γ and Δ, respectively, to $\mathbb{Q}$. The proof of Theorem 9.4A makes use of the $\mathbb{Q}$-linear transformation $\theta : \mathrm{Fun}(\Gamma, \mathbb{Q}) \to \mathrm{Fun}(\Delta, \mathbb{Q})$ given by

$$f^{\theta}(\delta) := \sum_{(\gamma,\delta)\in\Lambda} f(\gamma)$$

where $f \in \mathrm{Fun}(\Gamma, \mathbb{Q})$, $f^{\theta} \in \mathrm{Fun}(\Delta, \mathbb{Q})$, $\delta \in \Delta$ and $\gamma \in \Gamma$.

Lemma 9.4A. *Let G be a group which acts on both Γ and Δ and leaves Λ invariant. If the mapping θ is injective then the number of orbits of G on Γ is no greater than the number of orbits of G on Δ.*

PROOF. Let $V \subset \mathrm{Fun}(\Gamma, \mathbb{Q})$ and $W \subset \mathrm{Fun}(\Delta, \mathbb{Q})$ denote the subspaces of functions constant on the orbits of G. Another way to say this is that $f \in V$ if and only if $f(\gamma) = f(\gamma^x)$ for all $x \in G$ and similarly for W. Thus the dimensions of V and W are the numbers of orbits of G on the sets Γ and Δ respectively. Now since Λ is G-invariant, the transformation θ maps V into W. Hence, if θ is injective $\dim(V) \leq \dim(W)$ and the result follows. $\square$

Theorem 9.4A. *Let G be a group acting on a set Ω.*

(i) *If k and m are integers such that $0 \leq m \leq k$ and $k + m \leq |\Omega|$ then G has at least as many orbits on $\Omega^{\{k\}}$ as it has on $\Omega^{\{m\}}$.*

(ii) *If G is k-homogeneous and $0 < 2k \leq |\Omega| + 1$ then G is m-homogeneous for all m with $0 < m \leq k$. In particular, G is transitive.*

PROOF. (i) We shall apply Lemma 9.4A to $\Gamma = \Omega^{\{m\}}$ and $\Delta = \Omega^{\{k\}}$, and

$$\Lambda := \left\{(T, S) \mid T \in \Omega^{\{m\}}, S \in \Omega^{\{k\}} \text{ and } T \subseteq S\right\}.$$

Clearly, the property (9.4) defined above holds for Λ, so (i) follows from Lemma 9.4A provided we can show that the corresponding linear transformation θ has kernel 0. Equivalently, we must show that if f is a function from $\Omega^{\{m\}}$ into $\mathbb{Q}$, then the condition:

$$\sum_{T \in \Omega^{\{m\}},\ T \subseteq S} f(T) = 0 \quad \text{for all } S \in \Omega^{\{k\}} \tag{9.5}$$

implies that $f = 0$.

We prove this implication as follows. Suppose that condition (9.5) holds. For any finite subsets R, S of Ω with $R \subseteq S$ we define

$$g(R, S) := \sum_{T \in \Omega^{\{m\}},\ R \subseteq T \subseteq S} f(T).$$

Observe that g has the following two properties:

(a) $g(\emptyset, S) = 0$ for all S with $|S| \geq k$. Indeed this is true when $|S| = k$ by (9.5), and the general case, when $|S| = n$, say, follows from the easy identity:

$$\binom{n}{k} g(\emptyset, S) = \sum_{T \subseteq S,\ |T| = k} g(\emptyset, T);$$

(b) for any $\alpha \in \Omega$, $g(R, S) = g(R \setminus \{\alpha\}, S) - g(R \setminus \{\alpha\}, S \setminus \{\alpha\})$ since the left hand side is a sum of $f(T)$ over just those m-sets T which contain $R \setminus \{\alpha\}$ and are not disjoint from $\{\alpha\}$.

Now a simple induction on $|R|$ using properties (a) and (b) shows that $g(R, S) = 0$ whenever $R \subseteq S$ and $|S \setminus R| \geq k$. In particular, if $T \in \Omega^{\{m\}}$ then for any $S \in \Omega^{\{t+m\}}$ such that $T \subseteq S$, we have $f(T) = g(T, S) = 0$. Thus $f = 0$ and (i) is proved.

(ii) This follows immediately from (i) and the fact that a 1-homogeneous group is transitive. □

Exercises

9.4.6 Suppose that G acts k-homogeneously on Ω and that $1 \leq m \leq k$ with $k + m \leq |\Omega|$. Let Γ and Δ be subsets of Ω of sizes k and m

respectively. Show that $G_{\{\Gamma\}}$ has at least as many orbits on Γ as $G_{\{\Delta\}}$ has on Δ.

9.4.7 Under the hypotheses of the previous exercise, show that if $m \geq 2$ and $G_{\{\Delta\}}$ acts trivially on Δ then $G_{\{\Gamma\}}$ also acts trivially on Γ.

In the case of finite groups, there is a close relationship between multiply homogeneous groups and multiply transitive groups, as the following theorem [due to Livingstone and Wagner(1965) and Kantor (1972)] shows.

Theorem 9.4B. *Suppose that the group G is k-homogeneous on a finite set Ω where $2 \leq k \leq |\Omega|/2$. Then G is $(k-1)$-transitive and, with the following exceptions, G is k-transitve:*

(i) $k = 2$, $ASL_1(q) \leq G \leq A\Sigma L_1(q)$, $q \equiv 3 \pmod 4$;
(ii) $k = 3$, $PSL_2(q) \leq G \leq P\Sigma L_1(q)$, $q \equiv 3 \pmod 4$;
(iii) $k = 3$, $G = AGL_1(8), A\Gamma L_1(8), A\Gamma L_1(32)$;
(iv) $k = 4$, $G = PGL_2(8), P\Gamma L_2(8), P\Gamma L_2(32)$.

By contrast, in the infinite case, there are groups that are highly homogeneous but are not 2-transitive (Exercises 2.2.8 and 7.1.2). The highly homogeneous groups which are not highly transitive have been classified by Cameron (1976) as follows (compare with Examples 9.4.2 and 9.4.3).

Theorem 9.4C. *Suppose that the group G has a highly homogeneous action on a set Ω and that, for some k, the group G is k-transitive but not $k+1$-transitive. Then $k \leq 3$ and there is a relation ρ on Ω which is either a linear or a circular order such that every element of G either preserves or reverses ρ.*

We will not give proofs of these last two theorems, but will instead prove a theorem that is a special case of each. The result is due to J.P.J. McDermott.

Theorem 9.4D. *Let G be a 3-homogeneous group acting on a set Ω with $|\Omega| \geq 5$. Then, either G is 2-transitive or Ω is infinite and there exists a total order $\leq$ on Ω such that $G \leq \mathrm{Aut}(\Omega, \leq)$.*

PROOF. Theorem 9.4A shows that G is 2-homogeneous. Assume that G is not 2-transitive. Then G has exactly three orbitals: the diagonal consisting of all pairs (α, α) with $\alpha \in \Omega$ and two paired orbitals Γ and Δ where, for distinct points $\alpha, \beta \in \Omega$ one of the pairs $(\alpha, \beta), (\beta, \alpha)$ lies in Γ and the other lies in Δ. Since $|\Omega| \geq 4$, there exist distinct points α_0, β_0 and γ_0 in Ω such that (α_0, β_0) and (α_0, γ_0) lie in the same orbital, say Δ. Interchanging β_0 and γ_0 if necessary, we may also assume that $(\beta_0, \gamma_0) \in \Delta$.

We now define the relation $<$ on Ω by $\alpha < \beta \iff (\alpha, \beta) \in \Delta$ (and $\alpha \leq \beta \iff \alpha < \beta$ or $\alpha = \beta$). The relation $\leq$ is clearly preserved by G

and we claim that it is a total ordering on Ω. It is clear that we never have $\alpha < \alpha$ so $<$ is irreflexive. As noted above, if $\alpha, \beta \in \Omega$ are distinct then exactly one of $(\alpha, \beta), (\beta, \alpha)$ lies in Δ, hence either $\alpha < \beta$ or $\beta < \alpha$ and not both. It remains to show that $<$ is transitive.

Let α, β, γ be distinct points of Ω with $\alpha < \beta$ and $\beta < \gamma$. Then, by 3-homogeneity, there is an element $x \in G$ such that $\{\alpha, \beta, \gamma\}^x = \{\alpha_0, \beta_0, \gamma_0\}$. Also by the choice of α_0, β_0 and γ_0 we have $\alpha_0 < \beta_0, \beta_0 < \gamma_0$ and $\alpha_0 < \gamma_0$. Since G preserves the relation $<$, we have $\alpha^x = \alpha_0$, $\beta^x = \beta_0$ and $\gamma^x = \gamma_0$. But then $\alpha < \gamma$ since $\alpha_0 < \gamma_0$. Thus $<$ is transitive and so $\leq$ is a total order as asserted.

Finally, a finite total order has a trivial automorphism group (why?) and so Ω is infinite. This completes the proof of the theorem. □

Theorem 9.4A shows that every 2-homogeneous group is transitive, and Theorem 9.4B (i) lists the only finite 2-homogeneous groups which are not 2-transitive (they are all of odd order by Exercise 2.2.22 and so solvable). On the other hand, Theorem 9.4D shows us that every finite 3-homogeneous group is 2-transitive. Thus the characterization given in Theorem 9.4B (ii)–(iv) of finite k-homogeneous groups which are not k-transitive ($k \geq 3$) could be deduced from the list of 2-transitive groups of Sect. 7.7. Note, however, that Theorem 9.4B predates the classification of finite simple groups, so the original proof of this theorem did not follow these lines.

9.5 Automorphisms of Relational Structures

Recall that an *n-ary relation* ($n \geq 0$) on a set Ω is simply a subset of the Cartesian product $\Omega^n = \Omega \times \cdots \times \Omega$. We commonly refer to 1-ary, 2-ary and 3-ary relations as unary, binary and ternary relations, respectively. A relational structure is simply a set Ω together with a family of relations on Ω. This terminology was introduced in Sect. 2.4. In this section we give a construction which uses a class of finite relational structures (of a particular sort) to construct a countable relational structure with a large, and usually interesting, automorphism group.

In order to compare relational structures we introduce the "type" of a structure. Let Λ be a (possibly infinite) set, and associate to each $\lambda \in \Lambda$ a nonnegative integer n_λ. Then a *relational structure of type* $\langle n_\lambda \rangle_{\lambda \in \Lambda}$ is a set Ω together with an indexed family $\mathcal{R} = \langle \rho_\lambda \rangle_{\lambda \in \Lambda}$ where ρ_λ is an n_λ-relation on Ω. We denote the relational structure by $(\Omega; \mathcal{R})$ or $(\Omega; \langle \rho_\lambda \rangle_{\lambda \in \Lambda})$. We shall call this structure *finite* or *countable* when Ω is, respectively, finite or countably infinite.

EXAMPLE 9.5.1. A digraph can be represented as a relational structure of type $\langle 2 \rangle$. We take Ω as the set of vertices and $|\Lambda| = 1$, and the set of edges is the unique relation $\rho \subseteq \Omega^2$.

EXAMPLE 9.5.2. A partially order set $(\Omega, \leq)$ can also be represented as a relational structure of type $\langle 2 \rangle$. In this case the relation $\rho = \{(\alpha, \beta) \in \Omega^2 \mid \alpha \leq \beta\}$.

EXAMPLE 9.5.3. A ring $(R, +, \cdot)$ with unity 1 can be represented as a relational structure of type $\langle 1, 3, 3 \rangle$. We take $\Omega = R$ and the three relations: $\rho_1 = \{1\} \subseteq \Omega^1, \rho_2 = \{(a, b, c) \in R^3 \mid a + b = c\}$ and $\rho_3 = \{(a, b, c) \in R^3 \mid ab = c\}$.

Of course, in the last two examples, only part of the algebraic structure is reflected in terms of the relational structure. Further axioms are needed to ensure that we have a partial ordering or a ring.

EXAMPLE 9.5.4. If $\mathcal{S} = (\Omega; \mathcal{R})$ is any relational structure and Δ is an subset of Ω, then we have the *substructure* $\mathcal{U} = (\Delta; \mathcal{R}_\Delta)$ of the same type where $\mathcal{R}_\Delta$ is defined by restriction to Δ. Specifically, if $\mathcal{R} = \langle \rho_\lambda \rangle_{\lambda \in \Lambda}$, then $\mathcal{R}_\Delta := \langle \rho'_\lambda \rangle_{\lambda \in \Lambda}$ where $\rho'_\lambda := \rho_\lambda \cap \Delta^{n_\lambda}$. Note that, in Example 9.5.3 above, the substructures are not necessarily subrings.

Now suppose that $\mathcal{S} = (\Omega; \langle \rho_\lambda \rangle_{\lambda \in \Lambda})$ and $\mathcal{S}' = (\Omega'; \langle \rho'_\lambda \rangle_{\lambda \in \Lambda})$ are relational structures of the same type. Then an *embedding* $\phi : \mathcal{S} \to \mathcal{S}'$ is an injective mapping $\phi : \Omega \to \Omega'$ which "preserves" the relations; specifically, such that for each $\lambda \in \Lambda$:

$$(\alpha_1, \ldots, \alpha_{n_\lambda}) \in \rho_\lambda \iff (\phi(\alpha_1), \ldots, \phi(\alpha_{n_\lambda})) \in \rho'_\lambda.$$

The *image* of the embedding is the substructure of $\mathcal{S}'$ defined on the set $\phi(\Omega)$. A bijective embedding is an *isomorphism,* and in this case it easily verified that the inverse mapping $\phi^{-1} : \Omega' \to \Omega$ defines an isomorphism from $\mathcal{S}'$ to $\mathcal{S}$. As usual, when $\mathcal{S} = \mathcal{S}'$, these isomorphisms are call *automorphisms* of $\mathcal{S}$, and the set of all automorphisms forms a group $\mathrm{Aut}(\mathcal{S})$ under composition.

Exercise

9.5.1 Consider the examples above of partially ordered sets and rings with unity which are represented as relational structures. Suppose that ϕ is an isomorphism between two relational structures of type $\langle 2 \rangle$. If one of these structures is a partially ordered set, show that the relation for the other is also a partial ordering, and that ϕ is an order-preserving map between the sets. State and prove a similar result for rings with unity.

We are interested in relational structures $\mathcal{S}$ for which $\mathrm{Aut}(\mathcal{S})$ is large; in other words, where $\mathcal{S}$ has a high degree of symmetry. A relational structure $\mathcal{S}$ is called *homogeneous* if for each embedding ϕ of a finite substructure $\mathcal{U}$ of $\mathcal{S}$ into $\mathcal{S}$ there exists $\psi \in \mathrm{Aut}(\mathcal{S})$ such that ϕ equals the restriction $\psi_\mathcal{U}$

of ψ to $\mathcal{U}$. In other words, any embedding of a finite substructure of $\mathcal{S}$ into $\mathcal{S}$ can be extended to an automorphism of $\mathcal{S}$. The term "homogeneous" comes from model theory in logic. It has no relation to its use where we refer to "k-homogeneous" and "highly-homogeneous" permutation groups. Fortunately, the two uses do not often conflict, but you should be on your guard, as in the next example.

EXAMPLE 9.5.5. The relational structure $\mathcal{S} = (\mathbb{Q}, \leq)$ is homogeneous. Indeed, a finite substructure is essentially an ordered set of rationals $r_1 < r_2 < \ldots < r_k$ for some k. So an embedding of this finite substructure is a mapping $\phi : r_i \mapsto s_i$ where the s_i are rationals such that $s_1 < s_2 < \ldots < s_k$. We can extend ϕ to an order preserving permutation of $\mathbb{Q}$ by mapping the interval (r_i, r_{i+1}) to the interval (s_i, s_{i+1}) by a linear function, say, and mapping $(-\infty, r_1)$ to $(-\infty, s_1)$ and (r_k, ∞) to (s_k, ∞) by translations. Since every embedding of a finite substructure can be extended to an automorphism, the relational structure is homogeneous. ($\mathrm{Aut}(\mathbb{Q}, \leq)$ is also highly homogeneous in the sense of Sect. 2.1 and 9.4).

We shall give a construction and further examples of countable homogeneous relational structures with interesting automorphism groups below, but first we prove a simple criterion for recognizing when a countable relational structure is homogeneous.

Let $\mathcal{S}$ and $\mathcal{T}$ be two relational structures of the same type. We shall say that the *one-point extension property* holds for $\mathcal{S}$ into $\mathcal{T}$ when:

(1PX) if $\mathcal{U} \subset \mathcal{V}$ are finite substructures of $\mathcal{S}$ where $\mathcal{V}$ contains one more point than $\mathcal{U}$ does, then each embedding of $\mathcal{U}$ into $\mathcal{T}$ can be extended to an embedding of $\mathcal{V}$ into $\mathcal{T}$.

We now have the following useful result.

Theorem 9.5A. *Let $\mathcal{S}$ and $\mathcal{S}'$ be two countable relational structures of the same type, and suppose that (1PX) holds for $\mathcal{S}$ into $\mathcal{S}'$ and also holds for $\mathcal{S}'$ into $\mathcal{S}$. Then, for each embedding ϕ of a finite substructure $\mathcal{U}$ of $\mathcal{S}$ into $\mathcal{S}'$, there exists an isomorphism $\psi : \mathcal{S} \to \mathcal{S}'$ such that the restriction $\psi_{\mathcal{U}} = \phi$. In particular (take $\mathcal{U} = \emptyset$), $\mathcal{S}$ is isomorphic to $\mathcal{S}'$.*

We get an immediate corollary (take $\mathcal{S} = \mathcal{S}'$).

Corollary 9.5A. *If $\mathcal{S}$ is a countable relational structure and (1PX) holds for $\mathcal{S}$ into itself, then $\mathcal{S}$ is a homogeneous relational structure.*

Exercise

9.5.2 If $\mathcal{S}$ is any homogeneous relational structure, show that (1PX) holds for $\mathcal{S}$ into itself.

PROOF OF THEOREM 9.5A. Write $\mathcal{S} = (\Omega, \langle\rho_\lambda\rangle_{\lambda\in\Lambda})$ and $\mathcal{S}' = (\Omega', \langle\rho'_\lambda\rangle_{\lambda\in\Lambda})$. By hypothesis, each of these structures is countable; let α_i ($i \in \mathbb{N}$) and α'_i ($i \in \mathbb{N}$) be enumerations of Ω and Ω', respectively. The construction of the isomorphism ψ will be carried out by extending the definition of ϕ one point at a time using (1PX). However the construction is a little complicated because we need to use a "back and forth" argument to ensure that finally every point of $\mathcal{S}'$ is an image of some point of $\mathcal{S}$.

We proceed recursively to define two chains of finite substructures:

$$\mathcal{U}_0 \subset \mathcal{U}_1 \subset \mathcal{U}_2 \subset \dots \text{ in } \mathcal{S} \quad \text{and} \quad \mathcal{U}'_0 \subset \mathcal{U}'_1 \subset \mathcal{U}'_2 \subset \dots \text{ in } \mathcal{S}'$$

and embeddings:

$$\phi_k : \mathcal{U}_k \to \mathcal{S}' \quad \text{and} \quad \phi'_k : \mathcal{U}'_k \to \mathcal{S} \quad \text{for } k = 0, 1, \dots$$

These will satisfy the following conditions:

(i) $\mathcal{U}_0 = \mathcal{U}$ and $\phi_0 = \phi$;
(ii) $\mathcal{U}'_k$ is the image of ϕ_k and $\phi_k \circ \phi'_k$ is the identity on $\mathcal{U}_k$ ($k \geq 0$);
(iii) $\mathcal{U}_k$ and $\mathcal{U}'_k$ each contain one more point than $\mathcal{U}_{k-1}$ and $\mathcal{U}'_{k-1}$, ϕ_k is an extension of ϕ_{k-1}, and ϕ'_k is an extension of ϕ'_{k-1} ($k \geq 1$);
(iv) The points $\alpha_1, \dots, \alpha_m$ all lie in $\mathcal{U}_{2m}$, and the points $\alpha'_1, \dots, \alpha'_m$ all lie in $\mathcal{U}_{2m+1}$ ($k = 2m$ or $2m + 1$).

The construction proceeds as follows. For $k = 0$ we take $\mathcal{U}_0 = \mathcal{U}$ and take $\mathcal{U}'_0$ as the image of $\phi_0 = \phi$. Then (i), (ii) and (iv) are satisfied for $k = 0$. Now suppose that $k > 0$ and that (ii)–(iv) are satisfied for all smaller values of the index.

If $k = 2m$ is even, then we go "forth". Define $\mathcal{U}_k$ by adjoining α_i to $\mathcal{U}_{k-1}$ where α_i is the point of smallest index in Ω which does not already lie in $\mathcal{U}_{k-1}$. It follows from (iv) (for $k = 2m - 2$), that $i \geq m$. Since (1PX) holds for $\mathcal{S}$ into $\mathcal{S}'$, there exists a one-point extension $\phi_k : \mathcal{U}_k \to \mathcal{S}'$ of $\phi_{k-1} : \mathcal{U}_{k-1} \to \mathcal{S}'$. Denote the image of ϕ_k by $\mathcal{U}'_k$. Then ϕ_k gives an isomorphism of $\mathcal{U}_k$ onto $\mathcal{U}'_k$. Let ϕ'_k denote the inverse. It is now easy to check that (ii)–(iv) hold for $k = 2m$.

On the other hand, if $k = 2m+1$ is odd, then we go "back". In this case define $\mathcal{U}'_k$ by adjoining to $\mathcal{U}'_{k-1}$ the point α'_i of smallest index in Ω' which is not in $\mathcal{U}'_{k-1}$. Then proceed analogously to the case where k is even, but with the roles of $\mathcal{S}$ and $\mathcal{S}'$ reversed. Once again properties (ii)–(iv) can be proved to hold.

This describes the construction. Having made the construction we define $\psi : \mathcal{S} \to \mathcal{S}'$ by putting $\psi(\alpha) := \phi_k(\alpha)$ whenever $\phi_k(\alpha)$ is defined. The fact that ϕ_k is an extension of ϕ_j whenever $k > j$ (see (iii)), shows that this definition is consistent, and (iv) shows that ψ is defined for all $\alpha \in \Omega$. Now (iv) also shows that every finite subset of Ω is contained in all but a finite number of $\mathcal{U}_k$. In particular, for all $\alpha, \beta \in \Omega$ the condition $\psi(\alpha) = \psi(\beta)$ implies that $\phi_k(\alpha) = \phi_k(\beta)$ for some $k \geq 0$, and so $\alpha = \beta$; thus ψ is

injective. Similarly, for all $\lambda \in \Lambda$, and $\beta_1, \dots, \beta_{n_\lambda} \in \Omega$, we have $\beta_1, \dots, \beta_{n_\lambda}$ lying in $\mathcal{U}_k$ for some $k \geq 0$ and so

$$(\beta_1, \dots, \beta_{n_\lambda}) \in \rho_\lambda \iff$$
$$(\psi(\beta_1), \dots, \psi(\beta_{n_\lambda})) = (\phi_k(\beta_1), \dots, \phi_k(\beta_{n_\lambda})) \in \rho'_\lambda.$$

Thus ψ is embedding of $\mathcal{S}$ into $\mathcal{S}'$. Since ψ is surjective by (iv), we conclude that ψ is an isomorphism as asserted. □

Exercises

9.5.3 Consider $(\mathbb{Q}, \leq)$ with the usual ordering. Use Theorem 9.5A to show that $\mathrm{Aut}(\mathbb{Q}, \leq)$ is k-homogeneous for each $k \geq 1$.

9.5.4 Show that a countable totally ordered set $(\Omega, \leq')$ is order-isomorphic with $(\mathbb{Q}, \leq)$ if and only if:
 (i) the ordering is *dense* (for any pair of distinct points $\alpha, \beta \in \Omega$ with $\alpha \leq' \beta$ there exists $\gamma \neq \alpha$ or β such that $\alpha \leq' \gamma \leq' \beta$), and
 (ii) Ω has no largest or smallest element.
 For example, $(\mathbb{Q}, \leq)$ is order-isomorphic to the set of all rationals of the form $m/2^n$ ($m \in \mathbb{Z}, n \in \mathbb{N}$) with the usual ordering.

9.5.5 Let $\mathcal{T}$ be a tree with vertex set Ω. Show that $\mathcal{T}$ can be defined as a relational structure with a single ternary relation $\rho \subseteq \Omega^3$ where $(\alpha, \beta, \gamma) \in \rho$ if and only if β lies on the unique shortest path from α to γ in $\mathcal{T}$.

Theorem 9.5A, Corollary 9.5A and Exercise 9.5.2 together show that a countable homogeneous relational structure of a given type is determined, up to isomorphism, by the isomorphism classes of its finite substructures. The theorem below [due to R. Fraïssé (1954)] gives a useful criterion for the existence of homogeneous structures with specified classes of finite substructures.

Let $\mathbb{S}$ be a class of relational structures of a given type τ. We say that $\mathbb{S}$ is *closed under amalgamation* if: whenever $\mathcal{U}, \mathcal{V}_1, \mathcal{V}_2 \in \mathbb{S}$, and φ_1 and φ_2 are embeddings of $\mathcal{U}$ into $\mathcal{V}_1$ and $\mathcal{V}_2$, respectively, there exists $\mathcal{W} \in \mathbb{S}$, and embeddings ψ_1 and ψ_2 of $\mathcal{V}_1$ and $\mathcal{V}_2$, respectively, into $\mathcal{W}$ such that $\psi_1(\varphi_1(u)) = \psi_2(\phi_2(u))$ for all $u \in \mathcal{U}$. We call $\mathcal{W}$ an *amalgamation* of $\mathcal{V}_1$ and $\mathcal{V}_2$.

Theorem 9.5B. *Suppose that $\mathbb{S}$ is a class of finite relational structures of a fixed type τ, and that:*
 (i) *$\mathbb{S}$ is closed under isomorphism;*
 (ii) *$\mathbb{S}$ is closed under taking substructures;*
 (iii) *$\mathbb{S}$ contains only countably many nonisomorphic structures; and*
 (iv) *$\mathbb{S}$ is closed under amalgamation.*

Then there exists a countably infinite homogeneous structure $\mathcal{H}$ of type τ such that a finite structure $\mathcal{R}$ of type τ is isomorphic to a substructure of $\mathcal{H}$ if and only if $\mathcal{R} \in \mathbb{S}$.

PROOF. We shall show how to construct a countable relational structure $\mathcal{H}$ of type τ such that: each finite substructure of $\mathcal{H}$ lies in $\mathbb{S}$; each structure in $\mathbb{S}$ is isomorphic to a finite substructure of $\mathcal{H}$; and $(1PX)$ holds for $\mathcal{H}$ into itself. Then Corollary 9.5A shows that $\mathcal{H}$ is homogeneous as required.

Since all structures in $\mathbb{S}$ are finite, it follows from (iii) that there exists a countable family of pairs $(\mathcal{U}_i, \mathcal{V}_i)$ $(i \in \mathbb{N})$ from $\mathbb{S}$ such that: $\mathcal{U}_i \subseteq \mathcal{V}_i$ and $|\mathcal{V}_i| = |\mathcal{U}_i| + 1$; and, each pair $(\mathcal{U}, \mathcal{V})$ from $\mathbb{S}$ with $|\mathcal{V}| = |\mathcal{U}| + 1$ is isomorphic to exactly one of the pairs in this family. Using this we shall construct a chain $\mathcal{H}_0 \subseteq \mathcal{H}_1 \subseteq \mathcal{H}_2 \ldots$ in $\mathbb{S}$ such that each structure of size $\leq n$ in $\mathbb{S}$ is isomorphic to a substructure of $\mathcal{H}_n$. The union of this chain will be the required structure $\mathcal{H}$.

Take $\mathcal{H}_0 = \emptyset$. Assume that $n \geq 0$, and that we have already constructed $\mathcal{H}_n \in \mathbb{S}$; to construct $\mathcal{H}_{n+1}$ we proceed as follows. Since $\mathcal{H}_n$ is finite there are only finitely many embeddings $\mathcal{U}_i \to \mathcal{H}_n$, and by induction these include embeddings for all $\mathcal{U}_i$ of size n. We also have the embeddings $\mathcal{U}_i \to \mathcal{V}_i$, so by a series of successive amalgamations (and use of (iv) and (i)) we obtain $\mathcal{H}_{n+1} \in \mathbb{S}$ with $\mathcal{H}_{n+1} \supseteq \mathcal{H}_n$ such that each embedding of the form $\mathcal{U}_i \to \mathcal{H}_n \subseteq \mathcal{H}_{n+1}$ can be extended to an embedding $\mathcal{V}_i \to \mathcal{H}_{n+1}$. A simple induction argument (using (ii)), shows that every structure of size $\leq n+1$ in $\mathbb{S}$ is isomorphic to a substructure of $\mathcal{H}_{n+1}$, and that $(1PX)$ holds for $\mathcal{H}_{n+1}$ into itself for pairs $(\mathcal{U}, \mathcal{V})$ when $|\mathcal{U}| \leq n$.

Finally define $\mathcal{H} := \bigcup_{n \geq 0} \mathcal{H}_n$ (with the induced relational structure). It is then straightforward to verify that $\mathcal{H}$ has the properties asserted. □

EXAMPLE 9.5.6. (An infinite group which is $(k-1)$- but not k-transitive) A *k-hypergraph* consists of a set Ω (of *vertices*) together with a set $E \subseteq \Omega^{\{k\}}$ of *hyperedges*. Alternatively, the k-hypergraph can be defined via a k-ary relation ρ on Ω where $(\alpha_1, \ldots, \alpha_k) \in \rho \iff \{\alpha_1, \ldots, \alpha_k\} \in E$. A 2-hypergraph is simply a graph. Fix $k \geq 2$, and let $\mathbb{S}$ be the class of all finite k-hypergraphs. It is easy to verify that the conditions of Theorem 9.5B hold for $\mathbb{S}$ (see Exercise 9.5.6), and so there exists a (unique) countable homogeneous k-hypergraph $\mathcal{H}$. Put $G := \mathrm{Aut}(\mathcal{H})$. Then G is not k-transitive, because G preserves k-hyperedges of $\mathcal{H}$. On the other hand, any two k-hypergraphs of size $k-1$ are isomorphic because they have no hyperedges, and so G is $(k-1)$-transitive by the homogeneity of $\mathcal{H}$ (Theorem 9.5A).

Exercises

9.5.6 Show that the hypotheses of Theorem 9.5B hold for the class of k- hypergraphs. [*Hint:* To prove (iv) note that if $\mathcal{V}_1$ and $\mathcal{V}_2$ are k-hypergraphs, and $\mathcal{U} = \mathcal{V}_1 \cap \mathcal{V}_2$, then the union of $\mathcal{V}_1$ and $\mathcal{V}_2$ forms a k-hypergraph which is an amalgamation of $\mathcal{U} \to \mathcal{V}_1$ and $\mathcal{U} \to \mathcal{V}_2$.]

9.5.7 A graph is *triangle-free* if it does not contain a set of three pairwise adjacent points. Show that the class $\mathbb{T}$ of all triangle-free finite graphs satisfies the four conditions of Theorem 9.5B, and hence there exists a countable homogeneous triangle-free graph.

9.5.8 Define the infinite graph $\mathcal{G}$ as the disjoint union of a countable number of complete graphs each on its own set of m vertices. Show that $\mathcal{G}$ is a homogeneous graph. Describe the finite subgraphs of $\mathcal{G}$.

9.6 The Universal Graph

In their study of random graphs in 1963, P. Erdös and A. Rényi noted a peculiar fact: if a graph with a countable number of vertices is chosen "at random", then with probability 1 we always obtain the same graph (up to isomorphism). They called this graph the *universal graph*, and it turns out to be an interesting example of a homogeneous relational structure with an interesting automorphism group. The automorphism group of the universal graph is primitive but not 2-transitive while the group of automorphisms and anti-automorphisms is 2-transitive. The group of almost-automorphisms (see Exercise 9.6.11) is highly transitive. In the context of the last section, the universal graph is a countable homogeneous structure.

We shall explain the result of Erdös and Rényi below, but shall first introduce what turns out to be a characterization of this graph. This is the *universal property* for an infinite graph $\mathcal{G}$:

(UP) For every pair Γ, Δ of disjoint finite sets of vertices of $\mathcal{G}$ there exists a vertex α of $\mathcal{G}$ such that α is adjacent to every vertex in Γ and is not adjacent to any vertex in Δ.

EXAMPLE 9.6.1. Consider the graph $\mathcal{G}$ with vertex set $\mathbb{N}$ in which two vertices m and n with $m < n$ are adjacent if and only if in the binary expansion $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_s}$ $(0 \leq k_1 < k_2 < \ldots < k_s)$ we have $k_i = m$ for some i. Then $\mathcal{G}$ satisfies (UP). Indeed, let Γ and Δ be disjoint finite subsets of $\mathbb{N}$, and let $d \in \mathbb{N}$ be a strict upper bound for $\Gamma \cup \Delta$. Then $n := \sum_{i \in \Gamma} 2^i + 2^d \notin \Gamma \cup \Delta$ is adjacent to each vertex in Γ and not adjacent to any vertex in Δ.

For alternative constructions of graphs which satisfy (UP), see Example 9.6.2 and Exercise 9.6.4, as well as Theorem 9.6B.

Theorem 9.6A. *Any two countable graphs which satisfy (UP) are isomorphic. Furthermore, any such graph is homogeneous (as a relational structure with a single binary relation).*

PROOF. By Theorem 9.5A and its Corollary, it is enough to show that whenever two countable graphs $\mathcal{G}$ and $\mathcal{G}'$ satisfy (UP) then the condition (1PX) given in Sect. 9.5 holds for $\mathcal{G}$ into $\mathcal{G}'$.

Suppose that $\phi : \mathcal{U} \to \mathcal{G}'$ is an embedding of a finite subgraph of $\mathcal{G}$ into $\mathcal{G}'$, and that $\mathcal{U}$ is extended to $\mathcal{V}$ by adding a further vertex α of $\mathcal{G}$. Then we can use (UP) to extend ϕ to an embedding $\phi* : \mathcal{V} \to \mathcal{G}'$ by choosing $\phi^*(\alpha)$ such that: for each vertex β of $\mathcal{U}$, $\phi^*(\alpha)$ is adjacent to $\phi(\beta)$ if and only if α is adjacent to β in $\mathcal{G}$. □

A countable graph which satisfies (UP) is called a *universal graph*. As the last theorem shows, the universal graph is unique up to isomorphism. The universal property can often be used to give rather simple proofs of facts about the universal graph.

EXAMPLE 9.6.2. The automorphism group of a countable universal graph contains an element which is a fixed point free cycle on the set of vertices. Indeed, consider the set GRC of all graphs $\mathcal{G}$ with vertex set $\mathbb{Z}$ which have automorphism groups containing the cycle $\alpha \mapsto \alpha + 1$. It is enough to show that GRC contains a universal graph. Let

$$\Phi(\mathcal{G}) := \{\alpha \in \mathbb{Z} \mid \alpha > 0 \text{ and } \alpha \text{ adjacent to } 0 \text{ in } \mathcal{G}\}.$$

Then $\Phi(\mathcal{G})$ completely determines the edges of $\mathcal{G}$: (α, β) is an edge in $\mathcal{G}$ if and only if $|\alpha - \beta| \in \Phi(\mathcal{G})$. Conversely, given any set Φ of positive integers there is a unique graph $\mathcal{G}$ in GRC with $\Phi(\mathcal{G}) = \Phi$. This gives a bijection between GRC and the set of all sets of positive integers. We shall show that there is a graph in GRC which is universal by constructing a suitable Φ recursively.

Enumerate the (countably many) pairs (Γ_k, Δ_k) $(k = 1, 2, \ldots)$ of finite disjoint subsets of $\mathbb{Z}$. Now construct a sequence of finite sets Φ_k of positive integers $(k = 1, 2, \ldots)$ as follows. At step 1, choose any integer $\alpha_1 \notin \Gamma_1 \cup \Delta_1$, and put $\Phi_1 := \{|\beta - \alpha_1| \mid \beta \in \Gamma_1\}$. In general, at step k $(k \geq 2)$, choose an integer α_k such that $|\beta - \alpha_k| > |\gamma - \alpha_i|$ for all $\beta \in \Gamma_k \cup \Delta_k$ and all $\gamma \in \Gamma_i \cup \Delta_i$ with $i < k$, and set $\Phi_k := \{|\beta - \alpha_k| \mid \beta \in \Gamma_k\}$. Finally, take Φ as the union of all Φ_k, and take $\mathcal{G} \in$ GRC such that $\Phi(\mathcal{G}) = \Phi$. It follows from the construction that $\mathcal{G}$ satisfies the universal property (UP); indeed, for $\Gamma = \Gamma_k$ and $\Delta = \Delta_k$ we can take $\alpha = \alpha_k$. □

The construction above shows that the automorphism group of the countable universal graph contains a transitive cycle. In fact, it has been shown by Cameron that the latter group contains $2^{\aleph_0}$ conjugacy classes of such cycles. Truss (1985) has determined the cycle structures of all elements of the automorphism group of the universal graph, and has proved that the group is simple.

Exercises

9.6.1 Show that every finite and every countable graph can be embedded into the countable universal graph (in the sense of relational structures).

9.6.2 Show that a tree $\mathcal{T}$ with a countable number of vertices is isomorphic to a spanning tree for the countable universal graph if and only if the tree has the property that for each finite set Δ of vertices of $\mathcal{T}$ there exists a vertex $\alpha \notin \Delta$ which is not adjacent in $\mathcal{T}$ to any vertex in Δ. Give an example of a countable tree which fails to have this property.

9.6.3 If (UP) holds for a graph $\mathcal{G}$, show that for any given Γ and Δ there are infinitely many vertices α to satisfy (UP) for Γ and Δ.

9.6.4 (For those who know some number theory) Let $\Omega = \{5, 13, 17, \ldots\}$ be the set of all primes of the form $4k + 1$, and consider the graph with vertex set Ω where vertices p and q are adjacent if and only if p is a quadratic residue (mod q). Show that this graph satisfies (UP).

9.6.5 Show that there are uncountably many isomorphism classes of countable graphs.

In contrast to the last exercise, we now show that in a suitable sense "almost all" (labelled) graphs on a countable vertex set are isomorphic to the universal graph. In order to make this statement precise we have to put a measure on the set $\mathrm{GR}(\Omega)$ of graphs on a fixed countable vertex set Ω. Let $\Omega^{\{2\}}$ be the set of 2-subsets of vertices. Then for each graph $\mathcal{G}$ with vertex set Ω there corresponds the set $E(\mathcal{G}) \subseteq \Omega^{\{2\}}$ consisting of all pairs of adjacent vertices. The mapping $\mathcal{G} \to E(\mathcal{G})$ is a bijection from $\mathrm{GR}(\Omega)$ onto the set of all subsets of $\Omega^{\{2\}}$. Since Ω is countable, $\Omega^{\{2\}}$ is also countable. Thus we can fix an enumeration of $\Omega^{\{2\}}$, and then define a mapping from $\mathrm{GR}(\Omega)$ onto the interval [0,1] via $\mathcal{G} \to \sum_{i=0}^{\infty} \epsilon_i(\mathcal{G})/2^i$ where $\epsilon_i(\mathcal{G})$ equals 1 if the vertices in the ith 2-subset of $\Omega^{\{2\}}$ are adjacent in $\mathcal{G}$, and equals 0 otherwise. This latter mapping is no longer injective. Two different binary expansions can represent the same real number, and this happens exactly when one of them ends in infinitely many zeros and the other in infinitely many ones; for example, $.10000\ldots = .01111\ldots$. However, no point in [0,1] is the image of more than two graphs.

Theorem 9.6B. *Under the mapping $GR(\Omega) \to [0,1]$ defined above, the image of the set of graphs which are not universal has (Lebesgue) measure 0 in $[0,1]$.*

Proof. For each pair Γ, Δ of disjoint finite subsets of Ω, and each $\alpha \in \Omega \setminus (\Gamma \cup \Delta)$, we define $J(\Gamma, \Delta, \alpha)$ to be the image in [0,1] of the set of graphs for which the condition in (UP) *fails* to hold, and put $J(\Gamma, \Delta) := \bigcap_{\alpha \notin \Gamma \cup \Delta} J(\Gamma, \Delta, \alpha)$. Then the image of the set of all graphs which are not universal is $\bigcup_{\Gamma,\Delta} J(\Gamma, \Delta)$. It is a standard result of measure theory that a countable union of sets of measure 0 is also of measure 0. On the other hand,

since Ω is countable, the number of pairs Γ, Δ of disjoint finite subsets of Ω is also countable. Thus it is enough to show that $J(\Gamma, \Delta)$ has measure 0 for every pair Γ, Δ.

To do this we first note that, for any specified list $\epsilon_1, \epsilon_2, \ldots, \epsilon_h$ from $\{0, 1\}$, the measure of the set of points $\xi \in [0, 1]$ whose first h binary digits are $\epsilon_1, \epsilon_2, \ldots, \epsilon_h$ is exactly 2^{-h}. From this it is easily seen by a simple summation that, for any k distinct indices $i_1, i_2, \ldots, i_h$, the measure of the set of points whose binary digits at these places have specified values is also 2^{-h}. More generally, if we permit m_1 different sequences of binary values at the places $i_1, i_2, \ldots, i_h$, and m_2 different sequences of values at a disjoint list of places $j_1, j_2, \ldots, j_k$, then the corresponding set of points ξ has measure $(m_1 2^{-h})(m_2 2^{-k})$.

Now let Γ and Δ be a fixed pair of disjoint finite sets, and enumerate the remaining points in Ω : $\alpha_1, \alpha_2, \ldots$. Define μ_n to be the measure of $\bigcap_{i=1}^{n} J(\Gamma, \Delta, \alpha_i) \supseteq J(\Gamma, \Delta)$. We complete the proof by showing that $\mu_n \to 0$ as $n \to \infty$. A graph $\mathcal{G}$ maps into $J(\Gamma, \Delta, \alpha_i)$ if and only if $\mathcal{G}$ does not have specified edges or nonedges between $|\Gamma| + |\Delta|$ particular pairs of vertices. This translates into the condition that $\xi \in J(\Gamma, \Delta, \alpha_i)$ if and only if ξ does not have specified binary digits at $|\Gamma| + |\Delta|$ particular places. Hence, from above, $J(\Gamma, \Delta, \alpha_i)$ has measure $1 - 2^{-|\Gamma|-|\Delta|}$. If $i \neq j$, then the places specified for $J(\Gamma, \Delta, \alpha_i)$ and $J(\Gamma, \Delta, \alpha_j)$ are disjoint. Thus induction on n shows that $\mu_n = \mu_{n-1}(1 - 2^{-|\Gamma|-|\Delta|}) = (1 - 2^{-|\Gamma|-|\Delta|})^n$. This shows that μ_n tends to 0 as $n \to \infty$, and so the theorem is proved. □

The previous theorem shows that, in a certain sense, "almost all" countable graphs are universal. We can sometimes use this theorem to show that the universal graph has a specified property $\mathcal{P}$ by proving that the set of graphs in $\mathrm{GR}(\Omega)$ with property $\mathcal{P}$ corresponds to a set of nonzero measure in [0,1].

Exercises

In the following exercises, $\mathcal{G}$ denotes the countable universal graph on the vertex set Ω, and $G := \mathrm{Aut}(\mathcal{G})$.

9.6.6 Show that $\mathcal{G}$ is isomorphic to any graph obtained from $\mathcal{G}$ by removing or adding a finite number of edges, or by deleting a finite number of vertices and the associated edges.

9.6.7 Show that G is primitive but not 2-transitive on Ω. Show that G is a subgroup of index 2 in a group which is 2-transitive on Ω.

9.6.8 Show that $|G| = 2^{\aleph_0}$.

9.6.9 Show that the stabilizer G_α of any vertex α is isomorphic to $G \times G$.

9.6.10 Prove that the only element of finite support in G is the identity.

9.6.11 Let $\mathrm{AAut}(\mathcal{G})$ denote the group of "almost automorphisms" of $\mathcal{G}$; that is, the permutations in $Sym(\Omega)$ which preserve the edge relation of

$\mathcal{G}$ for all but a finite number of vertex pairs. Show that $\mathrm{AAut}(\mathcal{G})$ is a highly transitive group containing G.

9.6.12 If the set Ω of vertices of $\mathcal{G}$ is partitioned into a finite number of subsets, show that the subgraph induced on at least one of these subsets is isomorphic to $\mathcal{G}$.

9.6.13 (Universal digraph) Adapt the property (UP) to digraphs. Show that countable digraphs satisfying this property exist, are unique up to isomorphism and are homogeneous. What other properties of the universal graph correspond to analogous properties of this universal digraph?

9.7 Notes

- Sect. 9.1: For general references to the Burnside Problem see Aidian (1979), Kostrikin (1990), Zelmanov (1991b) and Vaughan–Lee (1993). An elementary exposition of Golod (1964) is given in Fischer and Struik (1968).
- Theorem 9.1A: See Gupta (1989).
- Sect. 9.2: For general references to the material in this section see Serre (1980), Cohen (1989) and Cameron (1990).
- Theorem 9.2A: See Biggs (1989).
- Exercise 9.2.10: This result is known in combinatorics as "König's Lemma" (due to D. König in 1936).
- Lemma 9.2A and Theorem 9.2B: See Tits (1970).
- Sect. 9.3: For related papers see Adeleke (1988), Dixon (1990), Glass and McCleary (1991), Gunhouse (1992) and Hickin (1992).
- Exercises 9.3.1–2: See Cameron (1987).
- Exercises 9.4.3–4: See Cameron (1976).
- Theorem 9.4A: This theorem has an extensive history. Early proofs are due to Brown (1959), Livingstone and Wagner (1965) and Bercov and Hobby (1970). We have used the proof from Cameron (1976). See also Cameron (1978), (1981c), (1983a), (1983b) and (1990) page 53, Kantor (1972), Pouzet (1976) and Wielandt (1967b).
- Theorem 9.4B: See Livingstone and Wagner (1965) and Kantor (1972). See also Huppert and Blackburn (1982b).
- Exercises 9.4.7–8: See Cameron (1976).
- Theorem 9.4C: See Cameron (1976).
- Theorem 9.4D: This is an unpublished result of J.P.J McDermott; see Cameron (1990) Sect. 3.4.
- Sect. 9.5: For a general reference to this material see Cameron (1990).
- Theorem 9.5B: See Fraïssé (1954).
- Exercise 9.5.4: This is a classical result of G. Cantor.
- Sect. 9.6: The universal graph was originally defined in Erdös and Rényi (1963). In our exposition we have used Cameron (1990) as well as un-

published lecture notes of Cameron. Related papers included: Lachlan and Woodrow (1980), Mekler et al (1993), and Truss (1985), (1989) and (1991).

- Exercise 9.6.11: See Truss (1989) and (1991).
- Theorem 9.7B: See Erdös and Rényi (1963).

Appendix A

Classification of Finite Simple Groups

Every finite group can be built up of simple groups through successive extensions. The abelian simple groups are the groups of prime order. The finite nonabelian simple groups are broadly classified as: (i) the alternating groups A_n ($n \geq 5$); (ii) the simple groups of *Lie type*; and (iii) the *sporadic* simple groups. The *Classification of Finite Simple Groups* is the claim (based on many thousands of pages of research papers by dozens of mathematicians) that the only finite nonabelian simple groups are the presently known groups in classes (i)–(iii). The *Classification* was formally announced in Gorenstein (1979). Gorenstein et al (1994) is the first in a series of volumes from a project, presently under way, to present a coherent and accessible proof of the *Classification*.

The alternating groups are, of course, well understood. We briefly describe below the groups of Lie type and the 26 sporadic groups.

The Simple Groups of Lie Type

There are five families of *classical* finite simple groups of Lie type, each of which is obtained by factoring a suitable linear group by its centre (a group of scalars). These are the families of (projective) special linear groups, unitary groups, symplectic groups, and two families of orthogonal groups.

In Table A.1, q denotes a order of finite field and so is a prime power, and d represents the order of the centre which has been factored out. The groups are denoted by a common abbreviated notation where $PSL_n(q)$ is denoted by $L_n(q)$, $PSp_{2m}(q)$ by $S_{2m}(q)$, etc. (see Appendix B). We have $L_2(2) \cong S_3$, $L_2(3) \cong A_4$, $L_2(4) \cong L_2(5) \cong A_5$, $L_2(7) \cong L_3(2)$, $L_2(9) \cong A_6, L_4(2) \cong A_8, S_4(2) \cong S_6, U_4(2) \cong S_4(3)$, and $U_3(2)$ is solvable. With these exceptions the groups listed in Table A.1 are nonisomorphic nonabelian simple groups which are not isomorphic to alternating groups.

In addition to these families of classical groups, there are nine further families of groups of Lie type, parameterized by the prime power q, each of which is derived from a Lie algebra of specific dimension. With the

TABLE A.1. The Simple Groups of Lie Type

Name	Symbol	Order
Linear	$L_n(q)$	$q^{n(n-1)/2}\prod_{i=2}^{n}(q^i-1)/d$ where $d=\mathrm{GCD}(n,q-1),\ n\geq 2$
Unitary	$U_n(q)$	$q^{n(n-1)/2}\prod_{i=2}^{n}(q^i-(-1)^i)/d$ where $d=\mathrm{GCD}(n,q+1),\ n\geq 2$
Symplectic	$S_{2m}(q)$	$q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)/d$ where $d=\mathrm{GCD}(2,q-1),\ m\geq 3$
Orthogonal	$O_{2m+1}(q)$	$q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)/d$ where $d=\mathrm{GCD}(2,q-1),\ m\geq 2$
Orthogonal	$O_{2m}(q)$	$q^{m(m-1)}(q^m-\epsilon)\prod_{i=1}^{m-1}(q^{2i}-1)/d$ where $d=\mathrm{GCD}(4,q^m-\epsilon),\ m\geq 4, \epsilon=\pm 1$

notation introduced by C. Chevalley and R. Steinberg these are denoted: $G_2(q)$, $F_4(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, ${}^2B_2(q)$ $(q = 2^{2m+3})$, ${}^3D_4(q)$, ${}^2G_2(q)$ $(q = 3^{2m+3})$, ${}^2F_4(q)$ $(q = 2^{2m+3})$, and ${}^2E_6(q)$. The groups in the family ${}^2B_2$ are known as Suzuki groups, and the groups in the families ${}^2G_2$ and ${}^2F_4$ are known as Ree groups after their discoverers. Finally, there is the single exceptional group ${}^2F_4(2)'$ which is known as Tits' group.

Work of Chevalley in 1955 and of Steinberg in 1959 showed that all groups of Lie type can be defined and analyzed, more or less uniformly, by using the underlying Lie algebra structure. In particular, their groups of outer automorphisms can be constructed; these are all solvable and quite small [see Conway et al (1985)].

The Sporadic Simple Groups

These are the finite simple groups which do not fall into infinite families. Twenty six of them are known, and according to the *Classification* these are the only finite nonabelian simple groups which are not alternating or of Lie type. The five Mathieu groups were discovered in the middle of the last century, but the other sporadic simple groups where all discovered between 1964 and 1975. Table A.2 lists these groups with their orders and the date when the group was discovered (or predicted to exist). There are many interesting relations between these groups. In particular, the Mathieu group M_{24} contains all of the smaller Mathieu groups, and the Monster M contains (as sections) many of the other sporadic groups. The group of outer

TABLE A.2. The Sporadic Simple Groups

Name	Symbol	Order	Date
Mathieu	M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	1861
Mathieu	M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	1861
Mathieu	M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	1873
Mathieu	M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	1873
Mathieu	M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	1873
Janko	J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	1964
Hall–Janko	J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	1967
Suzuki	Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1967
Higman-Sims	HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	1967
McLaughlin	McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	1967
Conway	Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	1968
Conway	Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	1968
Conway	Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	1968
Janko	J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	1968
Fischer	Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1968
Held	He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	1969
Fischer	Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	1969
Fischer	Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	1969
Lyons	Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	1971
Rudvalis	Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	1972
O'Nan	$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	1973
Harada–Norton	HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	1974
Thompson	Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	1974
Baby Monster	B	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot$ $17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	1975
Monster	M	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot$ $19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	1975
Janko	J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	1975

automorphisms for each of the groups on this list has order at most 2, thus completing the verification of the Schreier Conjecture.

For further information about the classification, see Gorenstein (1979) and (1982), and Gorenstein et al (1994). Conway and Sloane (1988) and Conway et al (1985) give details about the sporadic groups. Thompson (1983) describes some of the history of the discovery of the sporadic groups. An interesting account of the 19th century search for finite simple groups can be found in Silvestri (1979).

Appendix B

The Primitive Permutation Groups of Degree Less than 1000

This appendix gives a list of all proper primitive permutation groups of degree less than 1000. Such a list is of interest in illustrating in concrete form the kinds of primitive groups which arise, in suggesting conjectures about primitive groups, and settling small exceptional cases which often occur in proofs. Earlier lists (of varying completeness and accuracy) of primitive groups of degree n have been published by Jordan (1872) for $n \leq 17$, by Burnside (1897) for $n \leq 8$, by Manning (in a long series of papers that appeared between 1906 and 1929) for $n \leq 15$, by Sims (1970) for $n \leq 20$ and by Pogorelov (1980) for $n \leq 50$. At about the same time as the list presented here originally appearing in Dixon and Mortimer (1988), a list covering the same range was published by Il'in and Takmakov (1986).

The permutation groups in the list are collected into *cohorts* where all groups in a cohort have the same socle and this socle has the same action in each group of the cohort. Thus an item in the list consists of a transitive action for a group H, the socle, on a set Ω and the normalizer N of H in $Sym(\Omega)$ where N acts primitively on Ω. It may happen that H itself is not primitive or that $\mathrm{soc}(N) \neq H$.

Consider, as an example, the entry for the simple group $T = PSL_2(7) \cong PSL_3(2)$ listed under type B in Table B.2. There are four cohorts. There are two primitive actions with socle T. Considering T as $PSL_2(7)$ there is a natural 2-transitive action of degree 8 with stabilizers isomorphic to 7:3. The image of T in S_8 has index 2 in its normalizer (which is isomorphic to $PGL_2(7)$), as indicated by the entry $H.2$ in this row. Taking T as $PSL_3(2)$ there is a natural 2-transitive action of degree 7 on the Fano plane $PG_2(2)$ with stabilizers isomorphic to S_4. The image of T in S_7 is self normalizing, indicated by the entry H in this row. As described in Example 4.6.1, T also has imprimitive actions of degrees 21 and 28 (on the flags and antiflags of $PG_2(2)$) and there is a group $T.2 \cong PGL_2(7)$ which is primitive in both cases. These actions are recorded with first entry $PSL_2(7).2$, the smallest primitive group containing the socle with this action.

The socle H is a direct power of some simple group T. The various possiblities are that the socle is simple, composite with product action,

composite with diagonal action or regular. We assign each of the cohorts to a type as in Table B.1 Each cohort of Types A–H has a simple socle. Some simple groups could appear under more than one of these headings; each is assigned to the earliest valid type. Tables B.2, B.3 and B.4 do not include the affine groups. In addition to the cohorts listed in these tables, there is a cohort of affine groups for each degree which is a prime power p^k $(k \geq 1)$; the socle is a regular elementary abelian p-group of order p^k, and the normalizer is $A\Gamma L_k(p)$ (see Sect. 2.8). All solvable primitive permutation groups are affine. Short (1992) lists the solvable primitive groups of degree less than 256 and discusses the general construction of primitive affine groups. Theorem 4.7B shows that there are no primitive groups with a regular nonabelian socle and degree less than $60^6 > 1000$.

Tables B.2 and B.3 lists the proper primitive groups of degree less than 1000 by socle. Table B.4 lists the cohorts by degree. A typical entry in Table B.4 is 136 : AB^2E^2F which records the fact that there are five cohorts of primitive groups of degree 136 of types A, B, E and F with two each of types B and E. Using this information, the cohorts themselves can be located in Table B.2.

There are 762 cohorts of proper primitive groups of degree less than 1000. There are 355 degrees listed in Table B.4. There are a further 158 degrees not listed which are prime powers greater than 3. For these degrees only type K affine cohorts arise. The remaining 486 degrees less than 1000 have only improper primitive groups.

Considerable detailed information about the subgroups and automorphisms of the finite simple groups is required to construct the tables. This kind of information has been accumulating for more than a century as a result of the efforts of a number of mathematicians. In particular, we

TABLE B.1. Types of Cohorts of Primitive Groups

Type	Socles	Number of Cohorts
A	Alternating groups	77
B	$PSL_2(q)$	240
C	$PSL_n(q), n > 2$	56
D	Unitary groups	34
E	Symplectic groups	28
F	Orthogonal groups	13
G	Other groups of Lie type	7
H	Sporadic simple groups	38
I	Composite socles: product action	74
J	Composite socles: diagonal action	5
K	Regular abelian groups	190

acknowledge the importance of Conway et al. (1985) as a major source of useful data. Tables B.2 and B.3 use an abbreviated notation for the classical groups: $L_n(q) = PSL_n(q)$, $S_n(q) = Sp_n(q)$, $U_n(q) = PSU_n(q)$, $O_n(q) = PSO_n(q)$ and D_n denotes the dihedral group of order n. Other symbols refer to other groups of Lie type and the sporadic groups (see Appendix A). For further details see Conway et al (1985) and Dixon and Mortimer (1988).

TABLE B.2. Primitive Groups Listed by Socle: Simple Socles
Note: The natural action of A_n and the affine groups are not listed.

Primitive group G	Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
Type A. Alternating Groups (excluding the natural action)				
A_5 Out $= 2$	6	D_{10}	$H.2$	2
	10	S_3	$H.2$	3
$A_6 = L_2(3^2)$ Out $= 2^2$	10	$3^2 : 4$	$H.2^2$	2
	15	S_4	$H.2 = S_6$	3
$A_6.2 = PGL_2(3^2)$	36	D_{20}	$H.2^2$	4
	45	D_{16}	$H.2^2$	5
A_7 Out $= 2$	15	$L_2(7)$	H	2
	21	S_5	$H.2$	3
	35	$(A_4 \times 3) : 2$	$H.2$	4
$A_7.2 = S_7$	120	$7 : 6$	$H.2$	7
A_8 Out $= 2$	15	$2^3 : L_3(2)$	H	2
	28	S_6	$H.2$	3
	35	$2^4 : (S_3 \times S_3)$	$H.2$	3
	56	$(A_5 \times 3) : 2$	$H.2$	4
$A_8.2 = S_8$	105	$2^4 : S_4$	$H.2$	5
	120	$L_3(2) : 2$	$H.2$	5

A_9 Out $= 2$	36	S_7	$H.2$	3
	84	$(A_6 \times 3) : 2$	$H.2$	4
	120	$L_2(8) : 3$	H	3
	126	$(A_5 \times A_4) : 2$	$H.2$	5
	280	$3^3 : S_4$	$H.2$	5
	840	$3^2 : 2A_4$	$H.2$	> 10
A_{10} Out $= 2$	45	S_8	$H.2$	3
	120	$(A_7 \times 3) : 2$	$H.2$	4
	126	$(A_5 \times A_5) : 4$	$H.2$	3
	210	$(A_6 \times A_4) : 2$	$H.2$	5
	945	$2^4 : S_5$	$H.2$	7
A_{11} Out $= 2$	55	S_9	$H.2$	3
	165	$(A_8 \times 3) : 2$	$H.2$	4
	330	$(A_7 \times A_4) : 2$	$H.2$	5
	462	$(A_6 \times A_5) : 2$	$H.2$	6
A_{12} Out $= 2$	66	S_{10}	$H.2$	3
	220	$(A_9 \times 3) : 2$	$H.2$	4
	462	$(A_6 \times A_6) : 2^2$	$H.2$	4
	495	$(A_8 \times A_4) : 2$	$H.2$	5
	792	$(A_7 \times A_5) : 2$	$H.2$	6
A_{13} Out $= 2$	715	$(A_9 \times A_4) : 2$	$H.2$	5
A_m, $13 \le m \le 45$, Out $= 2$	$\binom{m}{2}$	S_{m-2}	$H.2$	3
A_m, $13 \le m \le 19$, Out $= 2$	$\binom{m}{3}$	$(A_{m-3} \times 3) : 2$	$H.2$	4

TABLE B.2. (*Continued*)

Primitive group G		Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
Type B. Projective Groups, $L_2(q)$					
$L_2(2^3)$	Out = 3	9	$2^3 : 7$	$H.3$	2
		28	D_{18}	$H.3$	2
		36	D_{14}	$H.3$	3
$L_2(2^4)$	Out = 4	17	$2^4 : 15$	$H.4$	2
		68	$L_2(2^2)$	$H.4$	4
		120	D_{34}	$H.4$	4
		136	D_{30}	$H.4$	5
$L_2(2^5)$	Out = 5	33	$2^5 : 31$	$H.5$	2
		496	D_{66}	$H.5$	4
		528	D_{62}	$H.5$	5
$L_2(2^6)$	Out = 6	65	$2^6 : 63$	$H.6$	2
		520	$L_2(2^3)$	$H.6$	
$L_2(2^7)$	Out = 7	129	$2^7 : 127$	$H.7$	2
$L_2(2^8)$	Out = 8	257	$2^8 : 255$	$H.8$	2
$L_2(2^9)$	Out = 9	513	$2^9 : 511$	$H.9$	2
$L_2(3^3)$	Out = 6	28	$3^3 : 13$	$H.6$	2
		351	D_{28}	$H.6$	6

	378	D_{26}	$H.6$	7
	819	$A_4 = L_2(3)$	$H.6$	> 10
$L_2(3^4)$ Out $= 2 \times 4$	82	$3^4 : 40$	$H.(2 \times 4)$	2
	369	$L_2(3^2).2$	$H.4$	
$L_2(3^5)$ Out $= 10$	244	$3^5 : 121$	$H.10$	2
$L_2(3^6)$ Out $= 2 \times 6$	730	$3^6 : 364$	$H.(2 \times 6)$	2
$L_2(5^2)$ Out $= 2^2$	26	$5^2 : 12$	$H.2^2$	2
	65	$L_2(5).2$	$H.2$	4
	300	D_{26}	$H.2^2$	9
	325	D_{24}	$H.2^2$	11
$L_2(5^3)$ Out $= 6$	126	$5^3 : 62$	$H.6$	2
$L_2(5^4)$ Out $= 2 \times 4$	626	$5^4 : 312$	$H.(2 \times 4)$	2
$L_2(7) = L_3(2)$ Out $= 2$	7	S_4	H	2
	8	$7 : 3$	$H.2$	2
$L_2(7).2$	28	D_{12}	$H.2$	5
	21	D_{16}	$H.2$	4
$L_2(7^2)$ Out $= 2^2$	50	$7^2 : 24$	$H.2^2$	2
	175	$L_2(7).2$	$H.2$	
	980	A_5	$H.2$	> 10
$L_2(7^3)$ Out $= 6$	344	$7^3 : 171$	$H.6$	2
$L_2(11)$ Out $= 2$	11	A_5	H	2

TABLE B.2. (*Continued*)

Primitive group G	Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
	12	$11:5$	$H.2$	2
	55	D_{12}	$H.2$	6
$L_2(11).2$	55	S_4	$H.2$	6
	66	D_{20}	$H.2$	7
$L_2(11^2)$ Out $= 2^2$	122	$11^2:60$	$H.2^2$	2
	671	$L_2(11).2$	$H.2$	
$L_2(13)$ Out $= 2$	14	$13:6$	$H.2$	2
	78	D_{14}	$H.2$	7
	91	D_{12}	$H.2$	8
	91	A_4	$H.2$	8
$L_2(17)$ Out $= 2$	18	$17:8$	$H.2$	2
	102	S_4	H	8
	136	D_{18}	$H.2$	9
	153	D_{16}	$H.2$	10
$L_2(19)$ Out $= 2$	20	$19:9$	$H.2$	2
	57	A_5	H	4
	171	D_{20}	$H.2$	10
	190	D_{18}	$H.2$	11
$L_2(19).2$	285	S_4	$H.2$	> 10

$L_2(23)$	Out $= 2$	24	$23 : 11$	$H.2$	2
		253	S_4	H	> 10
		253	D_{24}	$H.2$	> 10
		276	D_{22}	$H.2$	> 10
$L_2(29)$	Out $= 2$	30	$29 : 14$	$H.2$	2
		203	A_5	H	8
		406	D_{30}	$H.2$	> 10
		435	D_{28}	$H.2$	> 10
$L_2(31)$	Out $= 2$	32	$31 : 15$	$H.2$	2
		248	A_5	H	9
		465	D_{32}	$H.2$	> 10
		496	D_{30}	$H.2$	> 10
		620	S_4	H	> 10
$L_2(37)$	Out $= 2$	38	$37 : 18$	$H.2$	2
		666	D_{38}	$H.2$	> 10
		703	D_{36}	$H.2$	> 10
$L_2(41)$	Out $= 2$	42	$41 : 20$	$H.2$	2
		820	D_{42}	$H.2$	> 10
		861	D_{40}	$H.2$	> 10
$L_2(43)$	Out $= 2$	44	$43 : 21$	$H.2$	2
		903	D_{44}	$H.2$	> 10
		946	D_{42}	$H.2$	> 10
$L_2(p), 47 \leq p \leq 997,$	Out $= 2$	$p + 1$	$p : (p - 1)/2$	$H.2$	2

TABLE B.2. (*Continued*)

Primitive group G	Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
$L_2(p^2), 13 \leq p \leq 31$, Out $= 2^2$	p^2+1	$p^2 : (p^2-1)/2$	$H.2$	2
Type C. Projective Groups, $L_n(q), n > 2$				
$L_3(3)$ Out $= 2$	13	$3^2 : 2S_4$	$H.2$	2
	144	$13 : 3$	$H.2$	6
	234	S_4	$H.2$	> 10
$L_3(3).2$	52	$3_+^{1+2} : D_8$	$H.2$	4
	117	$2S_4 : 2$	$H.2$	6
$L_3(2^2)$ Out $= D_{12}$	21	$2^4 : A_5$	$H.6$	2
	56	A_6	$H.2^2$	3
	120	$L_2(7)$	$H.2^2$	4
	280	$3^2.Q_8$	$H.D_{12}$	5
$L_3(2^2).3 = PGL_3(2^2)$	960	$7 : 3 \times 3$	$H.D_{12}$	> 10
$L_3(2^2).2$ (graph auto.)	105	$2^{2+4}.3.2$	$H.D_{12}$	4
	336	S_5	$H.D_{12}$	8
$L_3(5)$ Out $= 2$	31	$5^2 : GL_2(5)$	H	2
$L_3(5).2$	186	$5_+^{1+2}.[2^5]$	$H.2$	4
	775	$4S_5.2$	$H.2$	> 6
$L_3(7)$ Out $= S_3$	57	$7^2 : 2L_2(7) : 2$	$H.3$	2

$L_3(7).2$	456	$7_+^{1+2} : (3 \times D_8)$	$H.S_3$	4
$L_3(2^3)$ Out $= 6$	73	$2^6 : (7 \times L_2(2^3))$	$H.3$	2
$L_3(2^3).2$	657	$2^{3+6} : 7^2 : 2$	$H.6$	4
$L_3(3^2)$ Out $= 2^2$	91	$3^4 : GL_2(3^2)$	$H.2$	2
$L_3(3^2).2$	910	$3^{2+4} : 8^2 : 2$	$H.2^2$	4
$L_3(q), 9 \leq q = p^d \leq 31$	q^2+q+1	$p^{2d} : GL_2(q)$	$P\Sigma L_3(q)$	2
$L_4(3)$ Out $= 2^2$	40	$3^3 : L_3(3)$	$H.2$	2
	117	$U_4(2) : 2$	$H.2$	3
	130	$3^4 : 2(A_4 \times A_4).2$	$H.2^2$	3
$L_4(3).2$	520	$3_+^{1+4} : (2S_4 \times 2)$	$H.2^2$	
$L_4(2^2)$ Out $= 2^2$	85	$2^6 : GL_3(4)$	$H.2$	2
	357	$2^8 : (L_2(4) \times L_2(4)).3$	$H.2$	3
$L_4(5)$ Out $= D_8$	156	$5^3 : L_3(5)$	$H.4$	2
	806	$5^4 : 2.(L_2(5) \times L_2(5)).2$	$H.4$	3
$L_4(7)$ Out $= 2^2$	400	$7^3 : 3.L_3(7).3$	$H.2$	2
$L_4(2^3)$ Out $= 6$	585	$2^9 : GL_3(2^3)$	$H.3$	2
$L_4(3^2)$ Out $= 2 \times D_8$	820	$3^6 : (2 \times L_3(3^2))$	$H.D_8$	2
$L_5(2)$ Out $= 2$	31	$2^4 : L_4(2)$	H	2
	155	$2^6 : (S_3 \times L_3(2))$	H	3
$L_5(2).2$	465	$2_+^{1+6} : L_3(2) : 2$	$H.2$	5

TABLE B.2. (*Continued*)

Primitive group G	Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
	496	$L_4(2) : 2$	$H.2$	5
$L_5(3)$ Out $= 2$	121	$3^4 : L_4(3).2$	H	2
$L_5(2^2)$ Out $= 2^2$	341	$2^8 : GL_4(2^2)$	$H.2$	2
$L_5(5)$ Out $= 2$	781	$5^4 : GL_4(5)$	H	2
$L_6(2)$ Out $= 2$	63	$2^5 : L_5(2)$	H	2
	651	$2^8 : (L_2(2) \times L_4(2))$	H	3
$L_6(3)$ Out $= 2^2$	364	$3^5 : L_5(3)$	$H.2$	2
$L_7(2)$ Out $= 2$	127	$2^6 : L_6(2)$	H	2
$L_8(2)$ Out $= 2$	255	$2^7 : L_7(2)$	H	2
$L_9(2)$ Out $= 2$	511	$2^8 : L_8(2)$	H	2
Type D. Unitary Groups				
$U_3(3)$ Out $= 2$	28	$3_+^{1+2} : 8$	$H.2$	2
	36	$L_2(7)$	$H.2$	3
	63	$4.S_4$	$H.2$	4
	63	$4^2.S_3$	$H.2$	4
$U_3(2^2)$ Out $= 4$	65	$2^{2+4} : 15$	$H.4$	2
	208	$5 \times A_5$	$H.4$	5

	416	$5^2 : S_3$	$H.4$	6
$U_3(5)$ Out $= S_3$	50	A_7	$H.2$	3
	126	$5_+^{1+2} : 8$	$H.S_3$	2
	175	M_{10}	$H.2$	4
	525	$2S_5$	$H.S_3$	6
$U_3(5).2$	750	$L_2(7) : 2$	$H.2$	9
$U_3(7)$ Out $= 2$	344	$7^{1+2} : 48$	$H.2$	2
$U_3(2^3)$ Out $= 3 \times S_3$	513	$2^{3+6} : 21$	$H.(3 \times S_3)$	2
$U_3(3^2)$ Out $= 4$	730	$3^{2+4} : 80$	$H.4$	2
$U_4(2)$ Out $= 2$	27	$2^4 : L_2(4)$	$H.2$	3
	36	S_6	$H.2$	3
	40	$3_+^{1+2} : 2A_4$	$H.2$	3
	40	$3^3 : S_4$	$H.2$	3
	45	$2.(A_4 \times A_4).2$	$H.2$	3
$U_4(3)$ Out $= D_8$	112	$3^4 : L_2(3^2)$	$H.D_8$	3
	126	$U_4(2)$	$H.2^2$	3
	162	$L_3(4) : 2$	$H.2^2$	3
	280	$3_+^{1+4}.2S_4$	$H.D_8$	3
	540	$U_3(3)$	$H.D_8$	4
	567	$2^4 : A_6$	$H.2^2$	5
$U_4(2^2)$ Out $= 4$	325	$2^8 : L_2(2^4).3$	$H.4$	3
$U_4(5)$ Out $= 2^2$	756	$5^4 : L_2(5^2).4$	$H.2^2$	3

TABLE B.2. (*Continued*)

Primitive group G	Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
$U_5(2)$ Out $= 2$	165	$2_-^{1+6} : 3_+^{1+2} : 2A_4$	$H.2$	3
	176	$3 \times U_4(2)$	$H.2$	3
	297	$2^{4+4} : (3 \times A_5)$	$H.2$	3
$U_6(2)$ Out $= S_3$	672	$U_5(2)$	$H.S_3$	3
	693	$2_+^{1+8} : U_4(2)$	$H.S_3$	3
	891	$2^9 : L_3(4)$	$H.S_3$	4
Type E. Symplectic Groups				
Note: $S_2(q) = L_2(q)$, $S_4(2) = S_6$, $S_4(3) = U_4(2)$				
$S_4(2^2)$ Out $= 4$	85	$2^6 : (3 \times A_5)$	$H.2$	3
	120	$L_2(2^4) : 2$	$H.2$	3
	136	$(A_5 \times A_5) : 2$	$H.2$	3
$S_4(2^2).4$	425	$(2^2 \times 2^{2+4} : 3) : 12$	$H.4$	8
$S_4(5)$ Out $= 2$	156	$5_+^{1+2} : (4 \times A_5)$	$H.2$	3
	156	$5^3 : (2 \times A_5).2$	$H.2$	3
	300	$L_2(5^2) : 2$	$H.2$	4
	325	$2.(A_5 \times A_5).2$	$H.2$	4
$S_4(7)$ Out $= 2$	400	$7_+^{1+2} : (6 \times L_2(7))$	$H.2$	3
	400	$7^3 : (3 \times L_2(7)).2$	$H.2$	3

$S_4(2^3)$ Out $= 6$	585	$2^9 : (7 \times L_2(8))$	$H.6$	3
$S_4(3^2)$ Out $= 2^2$	820	$(3_+^{1+2})^2 : (8 \times L_2(9))$	$H.2^2$	3
	820	$3^6 : (4 \times L_2(9)).2$	$H.2^2$	3
$S_6(2)$ Out $= 1$	28	$U_4(2) : 2$	H	2
	36	S_8	H	2
	63	$2^5 : S_6$	H	3
	120	$U_3(3) : 2$	H	3
	135	$2^6 : L_3(2)$	H	4
	315	$2.[2^6] : (S_3 \times S_3)$	H	5
	336	$S_3 \times S_6$	H	5
	960	$L_2(8) : 3$	H	6
$S_6(3)$ Out $= 2$	364	$3_+^{1+4} : (2 \times S_4(3))$	$H.2$	3
$S_8(2)$ Out $= 1$	120	$O_8^-(2) : 2$	H	2
	136	$O_8^+(2) : 2$	H	2
	255	$2^7 : S_6(2)$	H	3
$S_{10}(2)$ Out $= 1$	496	$O_{10}^-(2) : 2$	H	2
	528	$O_{10}^+(2) : 2$	H	2

Type F. Orthogonal Groups

Note: $O_3(q) = L_2(q)$, $O_4^+(q) = L_2(q) \times L_2(q)$, $O_4^-(q) = L_2(q^2)$, $O_5(q) = S_4(q)$, $O_6^+(q) = L_4(q)$, $O_6^-(q) = U_4(q)$, $O_{2m+1}(2^k) = S_{2m}(2^k)$

$O_8^+(2)$ Out $= S_3$	120	$S_6(2)$	$H.2$	3
	135	$2^6 : A_8$	$H.2$	3

TABLE B.2. (*Continued*)

Primitive group G		Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
		960	A_9	$H.2$	4
$O_8^-(2)$	Out = 2	119	$2^6 : U_4(2)$	$H.2$	3
		136	$S_6(2)$	$H.2$	3
		765	$2^{3+6} : (L_3(2) \times 3)$	$H.2$	4
$O_{10}^+(2)$	Out = 2	496	$S_8(2)$	$H.2$	3
		527	$2^8 : O_8^+(2)$	$H.2$	3
$O_{10}^-(2)$	Out = 2	495	$2^8 : O_8^-(2)$	$H.2$	3
		528	$S_8(2)$	$H.2$	3
$O_7(3)$		351	$2U_4(3) : 2$	$H.2$	3
		364	$3^5 : S_4(3) : 2$	$H.2$	3
		378	$L_4(3) : 2$	$H.2$	3
Type G. Other Groups of Lie Type					
$Sz(2^3)$	Out = 3	65	$2^{2+3} : 7$	$H.3$	2
		560	$13 : 4$	$H.3$	9
$G_2(3)$	Out = 2	351	$U_3(3) : 2$	H	3
		364	$(3_+^{1+2} \times 3^2) : 2S_4$	H	4
		378	$L_3(2) : 2$	H	4
$G_2(2^2)$	Out = 2	416	J_2	$H.2$	3

$^3D_4(2)$ Out = 3	819	$2_+^{1+8} : L_2(8)$	$H.3$	4
Type H. Sporadic Simple Groups				
M_{11} Out = 1	11	M_{10}	H	2
	12	$L_2(11)$	H	2
	55	$M_9.2$	H	3
	66	S_5	H	4
	165	$M_8.S_3$	H	8
M_{12} Out = 2	12	M_{11}	H	2
	66	$M_{10}.2$	H	3
	144	$L_2(11)$	$H.2$	4
	220	$M_9 : S_3$	H	5
	396	$2 \times S_5$	$H.2$	7
	495	$2_+^{1+4}.S_3$	$H.2$	7
	495	$4^2 : D_{12}$	$H.2$	8
$M_{12}.2$	144	$L_2(11).2$	$H.2$	4
	880	$3_+^{1+2}.D_8$	$H.2$	> 10
J_1 Out = 1	266	$L_2(11)$	H	5
M_{22} Out = 2	22	$L_3(4)$	$H.2$	2
	77	$2^4 : A_6$	$H.2$	3
	176	A_7	H	3
	231	$2^4 : S_5$	$H.2$	4
	330	$2^3 : L_3(2)$	$H.2$	5
	616	M_{10}	$H.2$	5
	672	$L_2(11)$	$H.2$	6

TABLE B.2. (*Continued*)

Primitive group G	Degree	Stabilizer in G	Normalizer of the socle H	Rank of the normalizer
J_2 Out = 2	100	$U_3(3)$	$H.2$	3
	280	$3.PGL_2(9)$	$H.2$	4
	315	$2_-^{1+4} : A_5$	$H.2$	5
	525	$2^{2+4} : (3 \times S_3)$	$H.2$	6
	840	$A_4 \times A_5$	$H.2$	7
M_{23} Out = 1	23	M_{22}	H	2
	253	$L_3(4) : 2$	H	3
	253	$2^4 : A_7$	H	3
	506	A_8	H	4
HS Out = 2	100	M_{22}	$H.2$	3
	176	$U_3(5) : 2$	H	2
M_{24} Out = 1	24	M_{23}	H	2
	276	$M_{22} : 2$	H	3
	759	$2^4 : A_8$	H	4
McL Out = 2	275	$U_4(3)$	$H.2$	3
Co_3 Out = 1	276	$McL : 2$	H	2

TABLE B.3. Primitive Groups Listed by Socle: Composite Socles

Primitive Group G	Degree	Rank of the Normalizer
Type I. Composite Socles: Product Action, Theorem 4.1A case b(iii)		
$A_n \times A_n,\ 5 \leq n \leq 31$	n^2	3
$A_n \times A_n,\ 5 \leq n \leq 8$	$\binom{n}{2}^2$	6
$A_n \times A_n \times A_n,\ 5 \leq n \leq 9$	n^3	6
$A_5 \times A_5$	36	3
$A_6 \times A_6$	100	3
$A_7 \times A_7$	225	3
$A_8 \times A_8$	225	3
$A_5 \times A_5 \times A_5$	216	6
$A_5 \times A_5 \times A_5 \times A_5$	625	10
$L_2(q) \times L_2(q),\ 7 \leq q = p^d \leq 29, q \neq 9$	$(q+1)^2$	3
$L_2(7) \times L_2(7)$	49	3
$L_2(7) \times L_2(7) \times L_2(7)$	343	6
	512	6
$(L_2(7) \times L_2(7)).2^2$	441	10
	784	15
$L_2(8) \times L_2(8)$	784	3
$L_2(8) \times L_2(8) \times L_2(8)$	729	6
$L_2(11) \times L_2(11)$	121	3
$L_3(3) \times L_3(3)$	169	3
$L_3(4) \times L_3(4)$	441	3
$L_3(5) \times L_3(5)$	961	3
$L_5(2) \times L_5(2)$	961	3
$U_3(3) \times U_3(3)$	784	3
$U_4(2) \times U_4(2)$	729	6
$S_6(2) \times S_6(2)$	784	3
$M_{11} \times M_{11}$	121	3
	144	3
$M_{12} \times M_{12}$	144	3
$M_{22} \times M_{22}$	484	3
$M_{23} \times M_{23}$	529	3
$M_{24} \times M_{24}$	576	3
Type J. Composite Socles: Diagonal Action, Theorem 4.1A case b(ii)		
$A_5 \times A_5$	60	4
$L_2(7) \times L_2(7)$	168	5
$A_6 \times A_6$	360	5
$L_2(8) \times L_2(8)$	504	5
$L_2(11) \times L_2(11)$	660	6

TABLE B.4. Cohorts of Primitive Groups Listed by Degree

A Alternating Groups	B Projective Groups, $L_2(q)$	C Projective Groups, $L_n(q), n > 2$
D Unitary Groups	E Symplectic Groups	F Orthogonal Groups
G Other Groups of Lie Type	H Sporadic Groups	
I Composite Socles: Product Action	J Composite Socles: Diagonal Action	

Note: the alternating group A_n in its natural action and affine groups are not listed.

6: A	7: B	8: B	9: B	10: A^2	11: BH	12: BH^2
13: C	14: B	15: A^3	17: B	18: B	20: B	21: ABC
22: H	23: H	24: BH	25: I	26: B	27: D	28: AB^3DE
30: B	31: C^2	32: B	33: B	35: A^2	36: $A^2BD^2EI^2$	38: B
40: CD^2	41: B	44: B	45: A^2D	48: B	49: I^2	50: BD
52: C	54: B	55: AB^2H	56: AC	57: BC	60: BJ	62: B
63: CD^2E	64: I^2	65: B^2DG	66: ABH^2	68: B^2	72: B	73: C
74: B	77: H	78: AB	80: B	81: I^2	82: B	84: AB
85: CE	90: B	91: AB^2C^2	98: B	100: H^2I^3	102: B^2	104: B
105: A^2C	108: B	110: B	112: D	114: B	117: C^2	119: F
120: A^5BCE^3F	121: CI^3	122: B	125: I	126: A^2BD^2	127: C	128: B
129: B	130: C	132: B	133: C	135: EF	136: AB^2E^2F	138: B
140: B	144: CH^2I^4	150: B	152: B	153: AB	155: C	156: CE^2
158: B	162: D	164: B	165: ADH	168: BJ	169: I^2	170: B
171: AB	174: B	175: BD	176: DH^2	180: B	182: B	183: C
186: C	190: AB	192: B	194: B	196: I^2	198: B	200: B
203: B	208: D	210: A^2	212: B	216: I^2	220: AH	224: B
225: I^4	228: B	230: B	231: AH	234: BC	240: B	242: B
244: B^2	248: B	252: B	253: AB^2H^2	255: CE	256: I	257: B

258: B	264: B	266: H	270: B	272: B	273: C	275: H
276: ABH^2	278: B	280: $ACDH$	282: B	284: B	285: B	286: A
289: I^2	290: B	294: B	297: D	300: ABE	307: C	308: B
312: B	314: B	315: EH	318: B	324: I^2	325: $ABDE$	330: AH
332: B	336: CE	338: B	341: C	343: I^2	344: BD	348: B
350: B	351: $ABFG$	354: B	357: C	360: BJ	361: I	362: B
364: $AEFG$	368: B	369: B	374: B	378: $ABFG$	380: B	381: C
384: BC	390: B	396: H	398: B	400: CE^2I^2	402: B	406: AB
410: B	416: DG	420: B	422: B	425: E	432: B	434: B
435: AB	440: B	441: I^4	444: B	450: B	455: A	456: C
458: B	462: A^2B	464: B	465: ABC	468: B	480: B	484: I^2
488: B	492: B	495: AFH^2	496: AB^2CEF	500: B	504: BJ	506: H
510: B	511: C	512: I^2	513: BD	520: BC	522: B	524: B
525: DH	527: F	528: $ABEF$	529: I^2	530: B	540: D	542: B
548: B	553: C	558: B	560: AG	561: A	564: B	567: D
570: B	572: B	576: I^3	578: B	585: CE^2	588: B	594: B
595: A	600: B	602: B	608: B	614: B	616: H	618: B
620: B^2	625: I^2	626: B	630: A	632: B	642: B	644: B
648: B	651: C^2	654: B	657: C	660: BJ	662: B	666: AB
671: B	672: DH	674: B	676: I^2	678: B	680: A	684: B
692: B	693: D	702: B	703: AB	710: B	715: A	720: B
728: B	729: I^4	730: BD	734: B	740: B	741: A	744: B
750: D	752: B	756: D	757: C	758: B	759: H	762: B
765: F	770: B	774: B	775: C	780: A	781: C	784: I^7
788: B	792: A	798: B	806: C	810: B	812: B	816: A
819: BG	820: $ABCE^2$	822: B	824: B	828: B	830: B	840: ABH

(Continued)

TABLE B.4. (*Continued*)

841: I	842: B	854: B	858: B	860: B	861: AB	864: B
871: C	878: B	880: H	882: B	884: B	888: B	891: D
900: I^2	903: AB	908: B	910: C	912: B	920: B	930: B
938: B	942: B	945: A	946: AB	948: B	954: B	960: CEF
961: I^3	962: B	968: B	969: A	972: B	978: B	980: B
984: B	990: A	992: B	993: C	998: B		

References

Adeleke, S.A. 1988. Embeddings of infinite permutation groups in sharp, highly transitive, and homogeneous groups. *Proc. Edinburgh Math. Soc.* (2) 31, 169–178.

Adian, S. I. 1979. *The Burnside Problem and Identities in Groups*. Berlin: Springer–Verlag.

Alperin, J. 1965. On a theorem of Manning. *Math. Z.* 88, 434–435.

Alspach, B. 1968. A combinatorial proof of a conjecture of Goldberg and Moon. *Canad. Math. Bull.* 11, 655–661.

Apostol, T.M. 1976. *Introduction to Analytic Number Theory*. New York: Springer–Verlag.

Artin, E. 1957. *Geometric Algebra*. New York: Interscience. (reprinted: 1988. New York: Wiley).

Aschbacher, M. 1972. On doubly transitive permutation groups of degree $n \equiv 2 \pmod{p}$. *Illinois J.* 16, 276–278.

Aschbacher, M. and L.L. Scott. 1985. Maximal subgroups of finite groups. *J. Algebra* 92, 44–80.

Atkinson, M.D. (ed.) 1984. *Computational Group Theory*. London: Academic Press.

Babai, L. 1980. On the complexity of canonical labeling of strongly regular graphs. *SIAM J. Comput.*. 9, 212–216.

Babai, L. 1981. On the order of uniprimitive permutation groups. *Annals of Math.* 113, 553–568.

Babai, L. 1982. On the order of doubly transitive permutation groups. *Invent. Math.* 65, 473–484.

Babai, L. 1986. On the length of subgroup chains in the symmetric group. *Comm. Algebra* 14, 1729–1736.

Babai, L. 1989. The probability of generating the symmetric group. *J. Comb. Theory (A)* 52, 148–153.

Babai, L. and P. Erdös. 1982. Representations of group elements as short products. *Ann. Discrete Math.* 12, 27–30.

Babai, L. and A. Seress. 1987. On the degree of transitivity of permutation groups: a short proof. *J. Comb. Theory (A)* 45, 310–315.

Babai, L., P.J. Cameron and P.P. Pálfy. 1982. On the orders of primitive groups with restricted nonabelian composition factors. *J. Algebra* 79, 161–168.

Baddeley, R.W. 1993. Primitive permutation groups with a regular non-abelian normal subgroup. *Proc. London Math. Soc.* (3) 67, 547–595.

Baer, R. 1934. Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich. *Studia Math* 5, 15–17.

Ball, R.W. 1966. Maximal subgroups of symmetric groups. *Trans. Amer. Math. Soc.* 121, 393–407.

Bannai, E. and S. Iwasaki. 1974. A note on subdegrees of finite permutation groups, *Hokkaido Math. J.* 3, 95–97.

Baumgartner, J.E., S. Shelah and S. Thomas. 1993. Maximal subgroups of infinite symmetric groups. *Notre Dame J. Formal Logic* 34, 1–11.

Bercov, R.D. 1965. The double transitivity of a class of permutation groups. *Canad. J. Math.* 17, 480–493.

Bercov, R.D. and C.R. Hobby. 1970. Permutation groups on unordered sets. *Math. Z.* 115, 165–168.

Berkovic, Ja.G. 1989. On p-subgroups of finite symmetric and alternating groups. *Contemporary Math.* 93, 67–76.

Beth, Th., D. Jungnickel and H. Lenz. 1993. *Design Theory*. Cambridge: Cambridge Univ. Press.

Biggs, N.L. 1989. Proof of Serre's Theorem. *Discrete Math.* 78, 55–57.

Biggs, N.L. and A.T. White. 1979. *Permutation Groups and Combinatorial Structures*. London Math. Soc. Lect. Note Series no. 33, Cambridge: Cambridge Univ. Press.

Birch, B.J., R.G. Burns, S.O. Macdonald and P.M. Neumann. 1976. On the degrees of permutation groups containing elements separating finite sets. *Bull. Austral. Math. Soc.* 14, 7–10.

Blaha, K.D. 1992. Minimum bases for permutation groups: the greedy approximation, *J. Algorithms* 13, 297–306.

Bochert, A. 1889. Ueber die Transitivitätsgrenze der Substitutionengruppen, welche die Alternierende ihres Grades nicht einhalten. *Math. Ann.* 33, 572–583.

Bochert, A. 1897. Ueber die Classe der Transitiven Substitutionengruppen II. *Math. Ann.* 49, 133–144.

Bovey, J. 1980. The probability that some small power of a permutation has small degree. *Bull. London Math. Soc.* 12, 47–51.

Bovey, J., and A. Williamson. 1978. The probability of generating the symmetric group. *Bull. London Math. Soc.* 10, 91–96.

Brauer, R. 1941. On connections between the ordinary and modular characters of groups of finite order. *Ann. of Math.* (2) 42, 926–935.

Brazil, M., J. Covington, T. Penttila, C.E. Praeger and A.R. Woods. 1994. Maximal subgroups of infinite symmeric groups. *Proc. London Math. Soc.* (3) 68, 77–111.

Brown, M. 1959. Weak n-homogeneity implies weak $n-1$-homogeneity. *Proc. Amer. Math. Soc.* 10, 644–647.

de Bruijn, N.G. 1957. Embedding theorems for infinite groups. *Indag. Math.* 19, 560–569.

Buekenhout, F. 1988. On a theorem of O'Nan and Scott. *Bull. Soc. Math. Belg.* 40, 1–9.

Burnside, W. 1911. *Theory of Groups of Finite Order*. 2nd. ed. Cambridge: Cambridge Univ. Press. (reprinted: 1955, New York: Dover Publ.)

Butler, G. and J.J. Cannon. 1982. Computing in permutation and matrix groups, I. *Math. Comp.* 39, 663–670.

Butler, G. and J. McKay. 1983. The transitive groups of degree up to eleven. *Comm. Algebra* 11, 863–911.

Cameron, P.J. 1972. On groups with several doubly-transitive permutation representations. *Math. Z.* 128, 1–14.

Cameron, P.J. 1976. Transitivity of permutation groups on unordered sets. *Math. Z.* 148, 127–139.

Cameron, P.J. 1978. Orbits of permutation groups on unordered sets, I. *J. London Math. Soc.* (2) 17, 410–414.

Cameron, P.J. 1981a. Finite permutation groups and finite simple groups. *Bull. London Math. Soc.* 13, 1–22.

Cameron, P.J. 1981b. Normal subgroups of infinite multiply transitive permutation groups. *Combinatorica* 1, 343–347.

Cameron, P.J. 1981c. Orbits of permutation groups on unordered sets, II. *J. London Math. Soc.* (2), 23, 249–265.

Cameron, P.J. 1983a. Orbits of permutation groups on unordered sets, III. *J. London Math. Soc.* (2), 27, 229–237.

Cameron, P.J. 1983b. Orbits of permutation groups on unordered sets, IV. *J. London Math. Soc.* (2), 27, 238–247.

Cameron, P.J. 1987. Some permutation representations of a free group. *Europ. J. Combinatorics* 8, 257–260.

Cameron, P.J. 1990. *Oligomorphic Permutation Groups.* London Math. Soc. Lect. Note Series no. 152. Cambridge: Cambridge Univ. Press.

Cameron, P.J. and A.M. Cohen. 1992. On the number of fixed point free elements in a permutation group. *Discrete Math.* 106/107, 135–138.

Cameron, P.J. and K.W. Johnson. 1987. An investigation of countable B-groups. *Math. Proc. Camb. Philos. Soc.* 102, 223–231.

Cameron, P.J. and H.J. van Lint. 1991. *Designs, Graphs, Codes and their Links.* London Math. Soc. Student Texts no. 22. Cambridge: Cambridge Univ. Press.

Cameron, P.J., P.M. Neumann and D.N. Teague. 1982. On the degrees of primitive permutation groups. *Math. Z.* 180, 141–149.

Cameron, P.J., C.E. Praeger, J. Saxl and G.M. Seitz. 1983. On the Sims conjecture and distance transitive graphs. *Bull. London Math. Soc.* 15, 499–506.

Cameron, P.J., R. Solomon and A. Turull. 1989. Chains of subgroups in symmetric groups. *J. Algebra* 127, 340–352.

Carmichael, R. 1937. *Introduction to the Theory of Groups of Finite Order.* Boston: Ginn. (reprinted: 1956, New York: Dover Publ.)

Chapman, R.J. 1995. An elementary proof of the simplicity of the Mathieu groups M_{11} and M_{23}. *Amer. Math. Monthly* 102, 544–545.

Cohen, D.E. 1989. *Combinatorial Group Theory: a Topological Approach.* London Math. Soc. Student Texts no. 14. Cambridge: Cambridge Univ. Press.

Cole, F.N. 1894. List of the transitive substitution groups of ten and eleven letters. *Quart. J. Pure Appl. Math.* 27, 39–50.

Collins, M.J. 1990. Some infinite Frobenius groups. *J. Algebra* 131, 161–165.

Conway, J.H. 1969. A group of order 8,315,553,613,086,720,000. *Bull. London Math. Soc.* 1, 79–88.

Conway, J.H. 1971. Three Lectures on Exceptional Groups. *Finite Simple Groups.* (M. B. Powell and G. Higman eds.) New York: Academic Press.

Conway J.H. 1984. Hexacode and tetracode – MOG and MINIMOG. *Computational Group Theory.* (M.D. Atkinson, ed.) New York: Academic Press.

Conway, J.H. and N.J.A. Sloane. 1988. *Sphere Packings, Lattices and Groups.* New York: Springer-Verlag.

Conway, J.H., R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson. 1985. *An Atlas of Finite Simple Groups.* Oxford: Clarendon Press.

Cooperstein, B.N. 1978. Minimal degree for a permutation representation of a classical group. *Israel J. Math.* 30, 213–235.

Curtis, C.W., W.M. Kantor and G. Seitz. 1976. The 2-transitive permutation representations of the finite Chevalley groups. *Trans. Amer. Math. Soc.* 218, 1–57.

Curtis, R.T. 1976. A new combinatorial approach to M_{24}. *Math. Proc. Camb. Phil. Soc.* 79, 25–42.

Dickson, L.E. 1905. On Finite Algebras. *Nachr. kgl. Ges. Wiss. Göttingen.* 358–393.

Dixon, J.D. 1967. The Fitting subgroup of a linear solvable group. *J. Austral. Math. Soc.* 7, 417–424.

Dixon, J.D. 1969. The probability of generating the symmetric group. *Math. Z.* 110, 199–205.

Dixon, J.D. 1990. Most finitely generated permutation groups are free. *Bull. London Math. Soc.* 22, 222–226.

Dixon, J.D. and A. Majeed. 1988. Coset representatives for permutation groups. *Portug. Math.* 45, 61–68.

Dixon, J.D. and B.C. Mortimer. 1988. The primitive permutation groups of degree less than 1000. *Math. Proc. Camb. Philos. Soc.* 103, 213–238.

Dixon, J.D. and H.S. Wilf. 1983. The random selection of unlabeled graphs. *J. Algorithms* 4, 205–213.

Dixon, J.D., P.M. Neumann and S. Thomas. 1986. Subgroups of small index in infinite symmetric groups. *Bull. London Math. Soc.* 18, 580–586.

Dornhoff, L. 1969. The rank of primitive solvable permutation groups. *Math. Z.* 109, 205–210.

Dress, A.W. M., M.H. Klin and M.E. Muzichuk. 1992. On p-configurations with few slopes in the affine plane over $\mathbb{F}_p$ and a theorem of W. Burnside's. *Bayreuth Math. Schr.* 40, 7–19.

Droste, M. 1985. Structure of partially ordered sets with transitive automorphism groups. *Memoirs Amer. Math. Soc.* no. 57.

Easdown, D. and C.E. Praeger. 1988. On the minimal faithful degree of a finite group. *Bull. Austral. Math. Soc.* 38, 207–220.

Erdös, P. and A. Rényi. 1963. On random matrices. *Publ. Math. Inst. Hung. Acad. Sci.* 8, 455–461.

Evans, D.M. 1986. Subgroups of small index in infinite general linear groups. *Bull. London Math. Soc.* 18, 587–590.

Evans, D.M. 1987. A note on automorphism groups of countably infinite structures. *Arch. Math.* 49, 479–483.

Fein, B., W.M. Kantor and M. Schacher. 1981. Relative Brauer groups II. *J. reine angew. Math.* 328, 39–57.

Feit, W. and J.G. Thompson. 1963. Solvability of groups of odd order. *Pacific J. Math.* 13, 775–1029.

Finkelstein, L. and W.M. Kantor (eds.) 1993. *Groups and Computation.* DIMACS Series in Discrete Math. and Theoretical Comp. Sci. no. 11. Providence, RI: Amer. Math. Soc.

Fischer, I. and R.R. Struik. 1968. Nil algebras and periodic groups. *Amer. Math. Monthly* 75, 611–623.

Fisher, K.F. 1975. The polycyclic length of linear and finite polycyclic groups, *Canad. J. Math.* 26, 1002–1009.

Foulkes, H.O. 1963. On Redfield's group reduction functions. *Canad. J. Math.* 15, 272–284.

Foulser, D.A. 1969. Solvable permutation groups of low rank. *Trans. Amer. Math. Soc.* 134, 1–54.

Fraïssé, R. 1954. Sur l'extension aux rélations de quelques propriétés des orders. *Ann. Sci. Ecole Norm. Sup.* 71, 361–388.

Frobenius, G. 1902. Über primitive Gruppen des Grades n und der Klasse n–1, *S.b. Akad. Berlin* 455–459.

Gates, W.H. and C.H. Papadimitriou. 1979. Bounds for sorting by prefix reversal, *Discrete Math.* 27, 47–57.

Glass, A.M.W. and S.H. McCleary. 1991. Highly transitive representations of free groups and free products. *Bull. Austral. Math. Soc.* 43, 19–36.

Goldschmidt, D.M. and L.L. Scott. 1978. A problem of W.A. Manning on primitive permutation groups. *Math. Z.* 161, 97–100.

Golod, E.S. 1964. On nil-algebras and finitely approximable p-groups. *Izvest. Akad. Nauk. USSR Ser. Math.* 28, 273–276. [Russian]

Gorenstein, D. 1979. The classification of finite simple groups. *Bull. Amer. Math. Soc. (N.S.)* 1, 43–199.

Gorenstein, D. 1982. *Finite Simple Groups.* New York: Plenum.

Gorenstein, D., R. Lyons and R. Solomon. 1994. *The Classification of Finite Simple Groups.* Providence, RI: Amer. Math. Soc.

Grigorchuk, R.I. 1980. On the Burnside problem for periodic groups. *Functional Anal. Appl.* 14, 41–43.

Grün, O. 1945. Beiträge zur Gruppentheorie II. Über einen Satz von Frobenius. *J. Math.* 186, 165–169.

Gründhofer, Th. 1989. Sharply transitive linear groups and nearfields over p–adic fields. *Forum Math.* 1, 81–101.

Gunhouse, S.V. 1992. Highly transitive representations of free products on the natural numbers. *Arch. Math.* 58, 435–443.

Gupta, N.D. 1989. On groups in which every element has finite order. *Amer. Math. Monthly* 96, 297–308.

Gupta, N.D. and S. Sidki. 1983. On the Burnside problem for periodic groups. *Math. Z.* 182, 385–388.

Hall, M., Jr. 1954. On a theorem of Jordan. *Pacific J. Math.* 4, 219–226.

Hall, M., Jr. 1959. *The Theory of Groups.* New York: Macmillan.

Hall, M., Jr. 1962. Automorphisms of Steiner triple systems. *Proc. Symp. Pure Math.* vol. VI. Providence, RI: Amer. Math. Soc. 47–66.

Hall, P. 1962. Wreath products and characteristically simple groups. *Proc. Camb. Philos. Soc.* 58, 170–184.

Hering, C. 1974. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geom. Dedic.* 2, 425–460.

Herstein, I.N. 1958. A remark on finite groups. *Proc. Amer. Math. Soc.* 9, 255–257.

Hickin, K.K. 1992. Highly transitive Jordan representations of free products. *J. London Math. Soc.* (2) 46, 81–91.

Higman, D.G. 1964. Finite permutation groups of rank 3. *Math. Z.* 86, 145–156.

Higman, D.G. 1967. Intersection matrices for finite permutation groups. *J. Algebra* 6, 22–42.

Higman, D.G. and C. Sims 1968. A simple group of order 44,352,000. *Math. Z.* 105, 110–113.

Higman, G. 1969. On the simple groups of D.G. Higman and C.C. Sims. *Illinois J. Math.* 13, 74–80.

Higman, G., B. H. Neumann and H. Neumann. 1949. Embedding theorems for groups. *J. London Math. Soc. (1)* 24, 247–254.

Hoffman, K. and R. Kunze. 1971. *Linear Algebra.* 2nd ed. Engelwood Cliffs, NJ: Prentice–Hall.

Hoffman, P.N. and J.F. Humphreys. 1992. *Projective Representations of the Symmetric Group.* Oxford: Clarendon Press.

Hoffmann, C.M. 1982. *Graph–Theoretic Algorithms and Graph Isomorphism* Lect. Notes Comp. Sci. no. 136. New York: Springer–Verlag.

Hughes, D.R. 1965. Extensions of designs and groups: projective, symplectic and certain affine groups. *Math. Z.* 89, 199–205.

Hughes, D.R. and F.C. Piper. 1985. *Design Theory.* Cambridge: Cambridge Univ. Press.

Huppert, B. 1957. Zweifach transitive auflösbare Permutationsgruppen. *Math. Z.* 68, 126–150.

Huppert, B. 1967. *Endliche Gruppen I.* Berlin: Springer–Verlag.

Huppert, B. and N. Blackburn. 1982a. *Finite Groups II.* New York: Springer–Verlag.

Huppert, B. and N. Blackburn. 1982b. *Finite Groups III.* New York: Springer–Verlag.

Il'in, V.I. and A.S. Takmakov. 1986. Primitive simple permutation groups of small degrees. *Algebra and Logic* 25, 167–171.

Itô, N. 1992. On cyclic tournaments. *Hokkaido Math. J.* 21, 273–277.

Ivanov, A.A., M.Kh. Klin, S.V. Tsaranov and S.V. Shpektorov. 1983. On the problem of computing the subdegrees of transitive permutation groups. *Russian Math. Surveys.* 38, 123–124.

Janko, Z. 1964. Finite groups with a nilpotent maximal subgroup. *J. Austral. Math. Soc.* 4, 449–451.

Jerrum, M. 1986. A compact representation for permutation groups. *J. Algorithms* 7, 60–78.

Jordan, C. 1870. *Traité des substitutions et des equations algébriques.* Paris: Gauthier–Villars. (reprinted: 1957, Paris: Albert Blanchard).

Jordan, C. 1871. Théorèmes sur les groupes primitifs. *J. Math. Pures Appl.* 16, 383–408.

Jordan C. 1872. Récherches sur les substitutions. *Liouville's J.* (2) 17, 355.

Jordan, C. 1873. Sur la limite de transitivité des groupes non–alternées. *Bull. Soc. Math. France* 1, 40–71.

Jordan, C. 1875. Sur la limité du degré des groups primitifs qui contiennent une substitution donnée. *J. reine angew. Math.* 79, 248–253.

Kaloujnine, L. 1948. La structure des p-groupes de Sylow des groupes symmétriques finis. *Ann. Sci. École Norm. Sup.* (3) 65, 235–276.

Kaloujnine, L. and M. Krasner. 1948. Le produit complet des groupes de permutations et le problème d'extension des groupes. *C. R. Acad. Sci. Paris* 227, 806–808.

Kantor, W.M. 1969. Jordan Groups. *J. Algebra* 12, 471–493.

Kantor, W.M. 1972. k–homogeneous groups. *Math. Z.* 124, 261–265.

Kantor, W.M. 1974. Primitive groups having transitive subgroups of smaller, prime power degree. *Israel J. Math.* 18, 141–143.

Kantor, W.M. 1979. Permutation representations of the finite classical groups of small degree or rank. *J. Algebra* 60, 158–168.

Kantor, W.M. 1985a. Some consequences of the classification of finite simple groups, *Finite Groups-Coming of Age.* Contemp. Math. no. 45. Providence, RI: Amer. Math. Soc. 159–173.

Kantor, W.M. 1985b. Sylow's theorem in polynomial time. *J. Comp. and Sys. Sci.* 30, 359–394.

Kantor, W.M. 1987. Primitive permutation groups of odd degree, and an application to finite projective planes. *J. Algebra* 106, 15–45.

Kantor, W.M. and R.A. Liebler. 1982. The rank 3 permutation representations of the finite classical groups. *Trans. Amer. Math. Soc.* 271, 1–71.

Karolyi, G., S.J. Kovacs and P.P. Palfy. 1990. Double transitive permutation groups with abelian stabilizers. *Aequationes Math.* 39 (1990) 161–166.

Karrass, A. and D. Solitar. 1956. Some remarks on the infinite symmetric group. *Math. Z.* 66, 64–69.

Karzel, H. 1965. Unendliche Dicksonsche Fastkörper. *Arch. Math.* 16, 247–256.

Kerber, A. 1986. Enumeration under finite group action: symmetry classes of mappings. *Combinatoire énumérative* (G. Labelle et P. Leroux, eds.) Lect. Notes in Math. no. 1234. Berlin: Springer–Verlag. 160–176.

Kerby, W. 1974. On infinite sharply multiply transitive groups. *Hamb. Math. Einzelschriften* (New Series) no. 6.

Klemm, M. 1975. Über die Reduktion von Permutations Moduln. *Math. Z.* 143, 113–117.

Klemm, M. 1977. Primitive Permutationsgruppen von Primzahlpotenzgrad. *Comm. in Algebra* 5, 193–205.

Knapp, W. 1981. An order bound for the point stabilizer of a primitive permutation group. *Arch. Math.* 36, 481–484.

Knuth, D.E. 1991. Notes on efficient representation of permutation groups. *Combinatorica* 11, 57–68.

Kostrikin, A.I. 1990. *Around Burnside.* Berlin: Springer–Verlag.

Kovács, L.G. 1986. Maximal subgroups in composite finite groups. *J. Algebra* 99, 114–131.

Kovács, L.G. 1989. Primitive subgroups of wreath products in product action. *Proc. London Math. Soc.* (3) 58, 306–322.

Kovács, L.G. and M.F. Newman. 1988. Generating transitive permutation groups. *Quarterly J. Math. Oxford* (2) 39, 361–372.

Kramer, E.S., S.S. Magliveras and R. Mathon. 1989. The Steiner systems $S(2,4,25)$ with non–trivial automorphism groups. *Discrete Math.* 77, 137–157.

Lachlan, A.H. and R.E. Woodrow. 1980. Countable ultrahomogeneous undirected graphs. *Trans. Amer. Math. Soc.* 262, 51–94.

Landau, E. 1909. *Handbuch der Lehre von der Verteilung der Primzahlen.* Leipzig: Teubner. (reprinted: 1953, New York: Chelsea).

Lang, S. 1993. *Algebra.* 3rd ed. Reading, MA: Addison–Wesley.

Lauchli, H. and P.M. Neumann. 1988. On linearly ordered sets and permutation groups of countable degree. *Arch. Math. Logic* 27, 189–192.

Lennox, J.C. and S.E. Stoneheuer. 1986. *Subnormal Subgroups of Groups.* Oxford: Oxford Univ. Press.

Leon, J.S. 1980. On an algorithm for finding a base and strong generating set for a group given by generating permutations. *Math. Comp.* 35, 941–974.

Leon, J.S. 1984. Computing automorphism groups of combinatorial objects. *Computational Group Theory* (M.D. Atkinson, ed.). London: Academic Press. 321–336.

Levingston, R. 1978. Primitive permutation groups containing a cycle of prime power length. *Bull. London Math. Soc.* 10, 256–260.

Levingston, R. and D.E. Taylor. 1976. The theorem of Marggraff on primitive permutation groups which contain a cycle. *Bull. Austral. Math. Soc.* 15, 125–128.

Lidl, R. and G.L. Muller. 1993. When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly* 100, 71–74.

Liebeck, M.W. 1982. Bounds for the orders of some transitive permutation groups. *Bull. London Math. Soc.* 14, 337–344.

Liebeck, M.W. 1983. Extensions of a theorem of Jordan on primitive permutation groups. *J. Austral. Math. Soc. (A)* 34, 155–171.

Liebeck, M.W. 1984a. On the orders of transitive permutation groups. *Bull. London Math. Soc.* 16, 523–524.

Liebeck, M.W. 1984b. On minimal degrees and base sizes of primitive groups. *Arch. Math. (Basel)* 43, 11–15.

Liebeck, M.W. 1986. The affine permutation groups of rank 3. *Bull. London Math. Soc.* 18, 165–172.

Liebeck, M.W. and J. Saxl. 1985a. The primitive permutation groups containing an element of large prime order. *J. London Math. Soc.* (2) 31, 237–249.

Liebeck, M.W. and J. Saxl. 1985b. The primitive permutation groups of odd degree. *J. London Math. Soc.* (2) 31, 250–264.

Liebeck, M.W. and J. Saxl. 1986. The finite primitive permutation groups of rank three. *Bull. London Math. Soc.* 18, 165–172.

Liebeck, M.W. and J. Saxl. 1991. Minimal Degrees of Primitive Permutation Groups, with an Application to Monodromy Groups of Covers of Riemann Surfaces. *Proc. London Math. Soc.* (3) 63, 266–314.

Liebeck, M.W., C.E. Praeger and J. Saxl. 1987. The classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra* 111, 365–383.

Liebeck, M.W., C.E. Praeger and J. Saxl. 1988a. On the O'Nan–Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. (A)* 44, 389–396.

Liebeck, M.W., C.E. Praeger and J. Saxl. 1988b. On the 2–closures of primitive permutation groups. *J. London Math. Soc.* 37, 241–252.

Livingstone, D. and A. Wagner, 1965. Transitivity of finite permutation groups on unordered sets. *Math. Z.* 90, 393–403.

Luks, E.M. 1987. Computing the composition factors of a permutation group in polynomial time. *Combinatorica* 7, 87–99.

Lüneberg, H. 1969. *Transitive Erweiterungen endlicher Permutationsgruppen.* Lect. Notes in Math. no. 84. Berlin: Springer–Verlag.

Lüneburg, H. 1980. *Translation Planes*. Berlin: Springer–Verlag.

Lüneberg, H. 1981. Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von $a^N - 1$. *Geometries and Groups* Lect. Notes in Math. no. 893. New York: Springer–Verlag. 219–222.

MacPherson, H.D. and P.M. Neumann. 1990. Subgroups of infinite symmetric groups. *J. London Math. Soc.* (2) 42, 64–84.

MacPherson, H.D. and C.E. Praeger. 1990. Maximal subgroups of infinite symmetric groups. *J. London Math. Soc.* (2) 42, 85–92.

Manning, W.A. 1921. *Primitive Groups, Part I.* Math. and Astron., vol. I. Palo Alto, CA: Stanford Univ. Press.

Massias, J.P., J.L. Nicolas and G. Robin. 1989. Effective bounds for the maximal order of an element in the symmetric group. *Math. Comp.* 53, 665–678.

Mathieu, E. 1861. Mémoire sur l'étude des functions des plusieurs quantités, sur le manière de les former et sur les subsitutions qui les laissent invariables. *J. Math. Pures Appl. (Liouville)* (2) 6, 241–323.

Mathieu, E. 1873. Sur la function cinq fois transitive de 24 quantités. *J. Math. Pures Appl. (Liouville)* (2) 18, 25–46.

Maurer, I. 1955. Les groupes de permutations infinies. *Gaz. Mat. Fiz. (A)* 7, 400–408 (Romanian).

McDonough, T.P. 1977. A permutation representation of a free group. *Quart. J. Math. Oxford* (2) 28, 353–356.

Mekler, A.H. 1986. Groups embeddable in the autohomeomorphisms of Q. *J. London Math. Soc.* (2) 33, 49–58.

Mekler, A.H., R. Schipperus, S. Shelah and J.K. Truss. 1993. The random graph and the automorphisms of the rational world. *Bull. London Math. Soc.* 25, 343–346.

Miller, G.A. 1899. On simple groups which can be represented as substitution groups that contain cyclical substitutions of prime degree. *Amer. Math Monthly* 6, 102–103 (= *Coll. Works*. 1, 419–420).

Miller, G.A. 1900. Sur plusiers groupes simples. *Bull. Soc. Math. de France* 28, 266–267 (= *Coll. Works* 2, 65–66).

Miller, W. 1987. The maximal order of an element in a finite symmetric group. *Amer. Math. Monthly* 94, 497–506.

Mills, W.H. 1953. On non-isomorphism of certain holomorphs. *Trans. Amer. Math. Soc.* 74, 428–443.

Möller, R.G. 1991. The automorphism groups of regular trees. *J. London Math. Soc.* (2) 43, 236–252.

Mortimer, B.C. 1980. The modular permutation representations of the known doubly transitive groups. *Proc. London Math. Soc.* (3) 41, 1–20.

Neumann, B.H. 1940. On the commutativity of addition. *J. London Math. Soc.* 15, 203–208.

Neumann, B.H. 1954. Groups covered by finitely many cosets. *Publ. Math. Debrecen* 3, 227–242.

Neumann, B.H. 1963. Twisted wreath products of groups. *Arch. Math.* 14, 1–6.

Neumann, P.M. 1972. Transitive permutation groups of prime degree. *J. London Math. Soc.* (2) 5, 202–208.

Neumann, P.M. 1974. Transitive permutation groups of prime degree. *Proc. Second Internat. Conf. Theory of Groups* (A. Dold and B. Eckmann, eds.) Springer Lect. Notes in Math. no. 372. New York: Springer–Verlag. 520–535.

Neumann, P.M. 1975a. The lawlessness of groups of finitary permutations. *Arch. Math. (Basel)* 26, 561–566.

Neumann, P.M. 1975b. Primitive permutation groups containing a cycle of prime-power length. *Bull. London Math. Soc.* 7, 298–299.

Neumann, P.M. 1976. The structure of finitary permutation groups. *Arch. Math. (Basel)* 27, 3–17.

Neumann, P.M. 1977. Finite permutation groups, edge–coloured graphs and matrices. *Topics in Groups Theory and Computation* (M.P.J. Curran, ed.). London: Academic Press. 82–118.

Neumannn, P.M. 1979. A lemma which is not Burnside's. *Math. Scientist* 4, 133–141.

Neumann, P.M. 1985a. Some primitive permutation groups. *Proc. London Math. Soc.* (3) 50, 265–281.

Neumann, P.M. 1985b. Automorphisms of the rational world. *J. London Math. Soc.* (2) 32, 439–448.

Neumann, P.M. 1987. Some algorithms for computing with finite permutation groups, *Proc. Groups – St. Andrews 1985* (E.F. Robertson and C.M. Campbell eds.) London Math. Soc. Lect. Notes no. 121. Cambridge: Cambridge Univ. Press. 59–92.

Neumann, P.M. and M.R. Vaughan–Lee. 1977. An essay on BFC groups. *Proc. London Math. Soc.* (3) 35, 213–237.

Neumann, P.M., G.A. Stoy and E.C. Thompson. 1994. *Groups and Geometry*. Oxford: Oxford Univ. Press.

Nicolas, J.L. 1967. Sur l'ordre maximum d'un élément dans la groupe S_n des permutations. *Acta. Arith.* (1967/68) 14, 315–332.

Novikov, P.S. and S.I. Adian. 1968. Infinite periodic groups I, II, III. *Izvest. Akad. Nauk. USSR Ser. Math.* 32, 212–244, 251–254, 709–731. [Russian]

Ol'shanskii, A.Yu. 1982. On the Novikov–Adian theorem. *Math. USSR Sbornik* 118 (160), 203–235, 287. [Russian]

O'Nan, M. 1973. Automorphisms of unitary block designs. *J. Algebra* 20, 495–511.

Pálfy, P.P. 1982. A polynomial bound for the orders of primitive solvable groups. *J. Algebra* 77, 127–137.

Passman, D.S. 1968. *Permutation Groups*. New York: Benjamin.

Pogorelov, B.A. 1980. Primitive permutation groups of small degrees, I and II. *Algebra and Logic* 19, 230–254 and 278–296.

Pólya, G. 1937. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen and Chemische Verbindungen. *Acta Math.* 68, 145–254.

Pouzet, M. 1976. Application d'une propriété combinatoire des parties d'un ensemble aux groupes et aux relations. *Math. Z.* 150, 117–134.

Praeger, C.E. 1977. Sylow subgroups of transitive permutation groups II. *J. Austral. Math. Soc. Ser. A* 23, 329–332.

Praeger, C.E. 1979. On elements of prime order in primitive permutation groups. *J. Algebra* 60, 126–157.

Praeger, C.E. 1990. Finite primitive permutation groups: a survey, *Groups – Canberra*. Lect. Notes in Math. no. 1456. Berlin: Springer–Verlag. 63–84.

Praeger, C.E. and J. Saxl. 1980. On the order of primitive permutation groups. *Bull. London Math. Soc.* 12, 303–307.

Pyber, L. 1993a. The orders of doubly transitive permutation groups, elementary estimates. *J. Combin. Theory Ser. A* 62, 361–366.

Pyber, L. 1993b. Asymptotic results for permutation groups. *Groups and Computation* (L. Finkelstein and W.M. Kantor, eds.), DIMACS Series in Discrete Math. and Theoretical Comp. Sci. no. 11. Providence, RI: Amer. Math. Soc. 197–219.

Pyber, L. 1995. The minimal degree of primitive permutation groups. *Handbook of Combinatorics* (R.L. Graham, M. Grötschel and L. Lovász eds.) Amsterdam: North-Holland (to appear).

Read, R.C. 1968. The use of S-functions in combinatorial analysis. *Canad. J. Math.* 20, 808–841.

Ree, R. 1961. A family of simple groups associated with the simple Lie algebra of type (G_2). *Amer. J. Math.* 83, 432–462.

Ree R. 1964. Sur une famille de groupes de permutation doublement transitif. *Canad. J. Math.* 16, 797–820.

Robinson, D.J.S. 1972. *Finiteness Conditions and Generalized Soluble Groups*. Berlin: Springer–Verlag.

Rotman, J.L. 1995. *An Introduction to the Theory of Groups*. 4th ed. Graduate Texts in Math. no. 148. New York: Springer–Verlag.

Royle, G.F. 1987. Transitive groups of degree twelve. *J. Symbolic Comput.* 4, 255–268.

Samuel, P. 1988. *Projective Geometry*. New York: Springer–Verlag.

Scott, L.L. 1980. Representations in characteristic p. *The Santa Cruz Conference on Finite Groups* (B. Cooperstein and G. Mason eds.), Proc. Sympos. Pure Math. no. 37. Providence, RI: Amer. Math. Soc. 319–331.

Scott, W.R. 1964. *Group Theory*. Englewood Cliffs, NJ: Prentice–Hall. (reprinted: 1987, New York: Dover Publ.)

Schreier, J. and S. M. Ulam. 1936. Über die Automorphismen der Permutationsgruppe der natürlichen Zahlenfolge. *Fund. Math.* 28, 258–260.

Schur, I. 1908. Neuer beweis eines satzes von W. Burnside. *Jahresbericht der Deutsch. Math. Ver.* 17, 171–176 (= *Gesammelte Abhandlungen I* 266–271).

Schur, I. 1933. Zur Theorie der einfach transitiven Permutationsgruppen. *Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Klasse* 598–623 (= *Gesammelte Abhandlungen III*, 266–291).

Schur, I. 1973. *Gesammelte Abhandlungen, I–III.* Berlin: Springer–Verlag.

Seager, S.M. 1987. The rank of a finite primitive solvable permutation group. *J. Algebra* 105, 389–394.

Seager, S.M. 1988. A bound on the rank of primitive solvable permutation groups. *J. Algebra* 116, 342–352.

Segal, D. 1974. A note on finitary permutation groups. *Arch. Math.* 25, 470–471.

Semmes, S.W. 1981. Endomorphisms of infinite symmetric groups. *Abstracts Amer. Math. Soc.* 2, 426.

Serre, J.P. 1980. *Trees*. New York: Springer–Verlag.

Shalev, A. 1994. On the fixity of linear groups. *Proc. London Math. Soc.* (3) 68, 265–293.

Shaw, R.H. 1952. Remark on a theorem of Frobenius. *Proc. Amer. Math. Soc.* 3, 970–972.

Shelah, S. and S.R. Thomas. 1988. Implausible subgroups of infinite symmetric groups. *Bull. London Math. Soc.* 20, 313–318.

Shelah, S. and S.R. Thomas. 1989. Subgroups of small index in infinite symmetric groups. *J. Symbolic Logic* 54, 95–99.

Sheppard, J.A.H. and J. Wiegold. 1963. Transitive permutation groups and groups with finite derived groups. *Math. Z.* 81, 279–285.

Short, M. 1992. *The primitive soluble permutation groups of degree less than 256*. Lect. Notes in Math. no. 1519. Berlin: Springer–Verlag.

Silvestri, R. 1979. Simple groups in the nineteenth century. *Arch. Hist. Exact Sci.* 20, 313–356.

Sims, C.C. 1967. Graphs and permutation groups. *Math. Z.* 95, 76–86.

Sims, C.C. 1970. Computational methods in the study of permutation groups. *Computational Problems in Abstract Algebra* (J. Leech, ed.) New York: Pergamon Press. 169–184.

Sims, C.C. 1978. Some group theoretic algorithms. *Topics in Algebra, Proceedings, Canberra, 1978*. Lect. Notes in Math. no. 697. New York: Springer–Verlag. 108–124.

Sims, C.C. 1994. *Computation With Finitely Presented Groups*. Cambridge Univ. Press, Cambridge.

Smith, M.S. 1976. On the isomorphism of two simple groups of order 44,352,000. *J. Algebra* 41, 172–174.

Snapper, E. and R.J. Troyer. 1971. *Metric Affine Geometry*. New York: Academic Press. (reprinted: 1989, New York: Dover Publ.).

Stoller, G. 1963. Example of a proper subgroup of S_∞ which has a set–transitivity property. *Bull. Amer. Math. Soc.* 69, 220–221.

Suzuki, M. 1960. A new type of simple groups of finite order. *Proc. Nat. Acad. Sci. U.S.A.* 46, 868–870.

Suzuki, M. 1962. On a class of doubly transitive groups. *Ann. Math.* 75, 105–145.

Szep, J. 1953. Bemerkung zu einem Satz von O. Ore. *Publ. Math. Debrecen* 3, 81–82.

Taylor, D.E. 1974. Unitary block designs. *J. Combin. Theory* Ser. A 16, 51–56.

Taylor, D.E. 1992. *The Geometry of the Classical Groups*. Sigma Series in Pure Math. Berlin: Helderman.

Thompson, J.G. 1959. Finite groups with fixed point free automorphisms of prime order. *Proc. Nat. Acad. Sci. U.S.A.* 45, 578–581.

Thompson, J.G. 1970. Bounds for orders of maximal subgroups. *J. Algebra* 14, 135–138.

Thompson, T.M. 1983. *From Error-Correcting Codes Through Sphere Packings to Simple Groups*. Carus Math. Monograph no. 21. Washington, D.C.: Math. Assoc. Amer.

Tits, J. 1952. Sur les groupes doublement transitifs continus. *Comment. Math. Helv.* 26, 203–224.

Tits, J. 1960. Les groupes simple de Suzuki et de Ree. *Séminaire Bourbaki*. no. 210.

Tits, J. 1962. Ovoides et groupes de Suzuki. *Arch. Math.* 13, 187–198.

Tits, J. 1970. Sur le groupe des automorphismes d'un arbre. *Essays on Topology and Related Topics (Mémoires dédiés à Georges de Rham)*. Berlin: Springer–Verlag.

Tomkinson, M.F. 1987. Groups covered by finitely many cosets or subgroups. *Comm. Algebra* 15, 845–855.

Truss, J.K. 1985. The group of the countable universal graph, *Math. Proc. Camb. Philos. Soc.* 98, 213–245.

Truss, J.K. 1989. The group of almost automorphisms of the countable universal graph. *Math. Proc. Camb. Philos. Soc.* 105, 223–236.

Truss, J.K. 1991. Infinite simple permutation groups – a survey. *Groups–St. Andrews 1989*. vol. 2 (C.M. Campbell and E.F. Robertson eds.). London Math. Soc. Lect. Note Ser. no. 160. Cambridge: Cambridge Univ. Press. 463–484.

Tsuzuku, T. 1982. *Finite Groups and Finite Geometries*. Cambridge Tracts in Math. no. 76. Cambridge: Cambridge Univ. Press.

Vaughan–Lee, M. 1993. *The Restricted Burnside Problem* (2nd ed.). Oxford: Clarendon Press.

Weiss, M. J. 1935. On simply transitive groups. *Bull. Amer. Math. Soc.* 40, 401–405.

Wiegold, J. 1974. Groups of finitary permutations. *Arch. Math.* 25, 466–469.

Wielandt, H. 1934. *Abschätzungen für den Grad einer Permutationsgruppppe von vorgeschreibenem Transitivitätsgrad*. Dissertation. Univ. Berlin.

Wielandt, H. 1935. Zur Theorie der einfach transitiven Permutationsgruppen. *Math. Z.* 63, 582–587.

Wielandt, H. 1958. Über die Existenz von Normalteilern in endlichen Gruppen. *Math. Nachr.* 18, 274–280.

Wielandt, H. 1959. Ein Beweis für die Existenz von Sylow Gruppen. *Arch. Math.* 10, 401–402.

Wielandt, H. 1960a. Über den Transitivitätsgrad von Permutationsgruppen. *Math. Z.* 74, 297–298.

Wielandt, H. 1960b. *Infinite Permutation Groups*. Lecture notes. Tübingen: Univ. Tübingen.

Wielandt, H. 1962. Subnormale Hüllen in Permutationsgruppen. *Math. Z.* 79, 381–388.

Wielandt, H. 1964. *Finite Permutation Groups*. New York: Academic Press.

Wielandt, H. 1967a. On automorphisms of doubly transitive permutation groups. *Proc. Internat. Conf. Theory of Groups, Canberra, 1965* (L.G. Kovács and B.H. Neumann, eds.) New York: Gordon and Breach.

Wielandt, H. 1967b. Endliche k–homogene Permutationsgruppen. *Math. Z.* 101, 142.

Wielandt, H. 1969. *Permutation Groups Through Invariant Relations and Invariant Functions*. Lecture notes. Columbus, OH: Ohio State Univ.

Wielandt, H. 1971a. *Subnormal Subgroups and Permutation Groups*. Lecture notes. Columbus, OH: Ohio State Univ.

Wielandt, H. 1971b. *Subnormale Untergruppen endlicher Gruppen*. Lecture notes. Tübingen: Univ. Tübingen.

Wielandt, H. 1974. Normalteiler in 3–transitiven Gruppen. *Math. Z.* 136, 243–244.

Wielandt, H. 1994. *Mathematische Werke – Mathematical Works (Vol. 1: Group Theory)* (B. Huppert and H. Schneider eds.). Berlin: Walter de Gruyter.

Wielandt, H. and B. Huppert. 1958. Normalteiler mehrfach transitiver Permutationsgruppen. *Arch. Math. (Basel)* 9, 18–26.

Williamson, A.G. 1973. On primitive permutation groups containing a cycle. *Math. Z.* 130, 159–162.

Witt, E. 1938a. Die 5–fach transitiven Gruppen von Mathieu. *Abh. Math. Sem. Univ. Hamburg* 12, 256–264.

Witt, E. 1938b. Uber Steinersche Systeme. *Abh. Math. Sem. Univ. Hamburg* 12, 265–275.

Wong, W.J. 1967. Determination of a class of primitive groups. *Math. Z.* 99, 235–246.

Yoshizawa, M. 1979. On infinite four–transitive permutation groups. *J. London Math. Soc.* (2) 19, 437–438.

Zaigier, D. 1990. A one-sentence proof that every prime $p \equiv 1 \bmod 4$ is a sum of two squares. *Amer. Math. Monthly* 97, 144.

Zassenhaus, H. 1935. Über transitive Erweiterungen gewisser Gruppen aus Automorphismen endlicher mehrdimensionalar Geometrien. *Math. Ann.* 111, 748–759.

Zassenhaus, H. 1936. Über endliche Fastkörper. *Abh. Math. Sem. Univ. Hamburg* 11, 187–220.

Zassenhaus, H. 1987. On Frobenius groups II: universal completion of nearfields of finite degree over a field of reference. *Result. Math.* 11, 317–358.

Zelmanov, E.I. 1991a. Solution of the restricted Burnside problem for groups of odd exponent. *Math. USSR Ixv.* 36, 41–60.

Zelmanov, E.I. 1991b. On the restricted Burnside problem. *Proc. Internat. Congress Math. (Kyoto, 1990)*. Tokyo: Math. Soc. Japan.

Znoiko, D.V. 1977. Automorphism Groups of Regular Trees. *Math. USSR Sb.* 32, 109–115.

Index

Graduate Texts in Mathematics

continued from page ii

119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.
121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*
124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part III.
125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course. *Readings in Mathematics*
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 BRIDGES. Computability: A Mathematical Sketchbook.
147 ROSENBERG. Algebraic K-Theory and Its Applications.
148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
149 RATCLIFFE. Foundations of Hyperbolic Manifolds.
150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
152 ZIEGLER. Lectures on Polytopes.
153 FULTON. Algebraic Topology: A First Course.
154 BROWN/PEARCY. An Introduction to Analysis.
155 KASSEL. Quantum Groups.
156 KECHRIS. Classical Descriptive Set Theory.
157 MALLIAVIN. Integration and Probability.
158 ROMAN. Field Theory.
159 CONWAY. Functions of One Complex Variable II.
160 LANG. Differential and Riemannian Manifolds.
161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
162 ALPERIN/BELL. Groups and Representations.
163 DIXON/MORTIMER. Permutation Groups.
164 NATHANSON. Additive Number Theory: The Classical Bases.
165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
167 MORANDI. Field and Galois Theory.
168 EWALD. Combinatorial Convexity and Algebraic Geometry.
169 BHATIA. Matrix Analysis.
170 BREDON. Sheaf Theory. 2nd ed.